IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, INC., Plaintiff, v. CISCO SYSTEMS, INC., Defendant.	CIVIL ACTION NO. 2:18cv94

*** * CONFIDENTIAL INFORMATION REDACTED * ***

TRANSCRIPT OF VIDEOCONFERENCE BENCH TRIAL PROCEEDINGS

Norfolk, Virginia

May 14, 2020

Volume 7A
Pages 898-1008

BEFORE: THE HONORABLE HENRY COKE MORGAN, JR.
United States District Judge

APPEARANCES:

KAUFMAN & CANOLES, P.C.
By: Stephen E. Noona
- and -
KRAMER LEVIN NAFTALIS & FRANKEL LLP
By: Paul J. Andre
Counsel for the Plaintiff

DUANE MORRIS LLP
By: Louis N. Jameson
Counsel for the Defendant

I N D E X

E X H I B I T S

(Proceedings commenced at 10:01 a.m.) 09:49:46

THE CLERK: Civil Action Number 2:18cv94, 10:01:46
Centripetal Networks, Inc. v. Cisco Systems, Inc. 10:01:50

For the plaintiff, Mr. Andre, Mr. Noona, are you 10:01:52
ready to proceed? 10:01:55

MR. NOONA: We are, Your Honor. 10:01:58

THE CLERK: For the defendants, Mr. Jameson, are you 10:01:59
ready to proceed? 10:02:02

MR. JAMESON: We are, Your Honor. 10:02:03

THE COURT: All right. We'll resume with the direct 10:02:06
examination of Dr. Cole. 10:02:11

ERIC COLE, Ph.D., called by the Plaintiff, having 10:02:16
been previously duly sworn, was examined and testified 10:02:16
further as follows: 10:02:16

DIRECT EXAMINATION (Resumed) 10:02:17

BY MR. ANDRE: 10:02:17

Q. Dr. Cole, if you would turn back on your video... 10:02:18

Thank you. 10:02:22

MR. ANDRE: May it please the Court? 10:02:22

BY MR. ANDRE: 10:02:22

Q. Dr. Cole, when we left off yesterday, we were talking 10:02:25
about the importance of Encrypted Traffic Analytics to 10:02:28
Cisco's new network, and we were showing Exhibit PTX-452. 10:02:33
I'd like to pull the front page of that up. 10:02:39

This is the June 20, 2017 press release where Cisco 10:02:45

announced the unveiling of the "Network of the Future." Do you recall that? 10:02:49 10:02:53

A. Yes, I do. 10:02:54

Q. And I'd like to turn your attention to Pages 2 -- bottom of Page 2 and top of Page 3 of this exhibit and look at the availability of this new technology. 10:02:56 10:03:02 10:03:07

Could you just tell the Court of the -- what's -- in this case when the Catalyst switches were going to be available. 10:03:14 10:03:17 10:03:20

A. The Catalyst switches are available June and July 2017, and then the Encrypted Traffic Analytics was scheduled for September 2017. 10:03:21 10:03:28 10:03:32

Q. And when was the DNA center going to be available? 10:03:33

A. The DNA center was available August 2017. 10:03:39

Q. Thank you. I'd like to show you what's been marked as PTX-963. 10:03:43 10:03:48

Dr. Cole, do you know what this document is? 10:03:52

A. Yes. This is a blog post for an executive platform that Cisco posts on where they're talking about their Encrypted Traffic Analytics. 10:03:54 10:04:00 10:04:04

MR. ANDRE: Your Honor, I'd like to admit PTX-963 into evidence. 10:04:04 10:04:11

MR. JAMESON: No objection. 10:04:12

THE COURT: Just a moment. 10:04:13

All right. PTX-963 will be admitted. 10:05:03

(Plaintiff's Exhibit PTX-963 was received in evidence.) 10:05:06 10:05:08

BY MR. ANDRE: 10:05:08

Q. Dr. Cole, looking at the title of PTX-963, the "Cisco Extends Encrypted Traffic Analytics to Nearly 50,000 Customers," did that influence your opinion as to whether or not the Encrypted Traffic Analytics was an important platform for Cisco? 10:05:09 10:05:14 10:05:19 10:05:21 10:05:25

A. Yes, it did. It shows that they're pushing this out to a large number of customers. And what is also particularly of interest is that first sentence: "Cisco has solved one of the biggest challenges facing the security industry." And, in my opinion, the way they were able to do this was by utilizing the '856 patent. 10:05:25 10:05:29 10:05:33 10:05:38 10:05:43 10:05:47

Q. And if you look down to that next paragraph, it says, "A breakthrough technology identifies malware in encrypted traffic without having to break the packets and inspect the contents." What is that referring to? 10:05:49 10:05:55 10:05:59 10:06:02

A. That's referring to a big challenge. As we talked about yesterday, the old way of dealing with encrypted traffic was to actually decrypt it each time, which created security issues, efficiency issues, and performance issues. So the hard challenge that everyone in the industry was trying to solve was how can you analyze encrypted traffic without actually decrypting it, and Centripetal, via the '856 patent, 10:06:03 10:06:09 10:06:11 10:06:15 10:06:20 10:06:22 10:06:27

was able to solve that problem. 10:06:31

Q. I want to show you a piece of a deposition that was played in open court on Friday of last week of a Cisco fellow by the name of David McGrew. 10:06:33 10:06:37 10:06:41

MR. ANDRE: And, Your Honor, this is PTX-1925. 10:06:45

THE COURT: This has been admitted? 10:06:47

MR. ANDRE: Not yet, Your Honor. I'd like to have it admitted. 10:06:52 10:06:55

THE COURT: PTX-1925 will be admitted. 10:07:04

(Plaintiff's Exhibit PTX-1925 was received in evidence.) 10:07:08 10:07:11

BY MR. ANDRE: 10:07:11

Q. Dr. Cole, looking at Mr. McGrew -- first of all, did you look at his transcript and follow his testimony on Friday? 10:07:11 10:07:18

A. Yes, I did. 10:07:20

Q. And could you describe what Mr. McGrew is discussing in this question and answer in Exhibit PTX-1925. 10:07:22 10:07:27

A. Yes. He was asked if he has an understanding of why Encrypted Traffic Analytics solution was developed, and essentially, he confirms everything I was saying; that more and more traffic is encrypted, and with encrypted traffic, it's very hard to find that malware communication, because the traditional methods of intrusive detection don't apply. 10:07:31 10:07:37 10:07:40 10:07:43 10:07:47 10:07:51

So they recognize that the old way of trying to analyze payload doesn't work when the adversary is encrypting 10:07:57 10:08:00

the communication, and he even goes on to say the older technologies don't work. So there's more and more encrypted traffic. Any organization that maintains information systems must be able to detect malware without decrypting the communication. 10:08:05 10:08:09 10:08:12 10:08:16 10:08:19

And he even goes on to say there's a cyber security need for a new -- a new -- defensive technique, which is ETA, which, in my opinion, is based off of the '856 patent. 10:08:20 10:08:23 10:08:29

Q. Now, Dr. Cole, you did some testing. You testified earlier yesterday you did testing in this case, correct? 10:08:34 10:08:37

A. Yes, I did. I acquired several of the products, and we went through, and we tested many scenarios to confirm how the products actually work and how they operate. 10:08:40 10:08:44 10:08:49

Q. And the demonstrative we have on the screen now of the testing setup, are those some of the routers and switches that you were testing that you got from Cisco? 10:08:50 10:08:56 10:08:58

A. Yes. You can see that these are stackable units, and these are physical units that we'll talk about later, have CPUs and memory. But these are actually computing devices, physical devices, and you can see that we have the different cables plugged into the routers and switches for testing. 10:09:01 10:09:06 10:09:11 10:09:17 10:09:19

Q. And I want to show you what has previously been admitted as PTX-408. 10:09:23 10:09:26

MR. ANDRE: But I want to admit a couple new pages, Your Honor. I want to admit Pages 144 and 149 of PTX-408, 10:09:28 10:09:30

and these are Bates numbers 481769 and 481774. 10:09:36

THE COURT: Say those numbers again. 10:09:48

MR. ANDRE: It's -- the Bates numbers? 10:09:52

THE COURT: Yes. 10:09:56

MR. ANDRE: The Bates numbers are 481769 and 481774. 10:09:57

And those should be in your binder, those two pages. 10:10:06

THE COURT: 769 and 774? 10:10:10

MR. ANDRE: That's correct. 10:10:17

THE COURT: All right. They'll be admitted. 10:10:18

(Plaintiff's Exhibit PTX-408, Pages 144 and 149, was 10:10:19

received in evidence.) 10:10:20

BY MR. ANDRE: 10:10:20

Q. Dr. Cole, could you explain to the Court what is being 10:10:21

shown of the testing of the Catalyst on the page ending in 10:10:23

Bates number 769, first. 10:10:27

A. Yes. As I mentioned yesterday, when I do my infringement 10:10:32

analysis, I look at many different components. I look at 10:10:35

documents, source code, testimony, and I actually do testing 10:10:37

of the products. And in order to confirm how the products 10:10:41

work, I utilize a tool called Wireshark, and Wireshark is a 10:10:44

sniffer. What this actually does is it lets me capture the 10:10:49

traffic going across the network so I can see exactly what's 10:10:53

happening and what's occurring on the system. 10:10:58

So I went in and turned on Encrypted Traffic 10:11:01

Analytics on the infringing devices. I then went in and made 10:11:05

some communication to a network badguy.com, and then I went in to search the traffic, saying would I be able to see the domain name, which is one of the components that's required for the patent, in the traffic stream. 10:11:10 10:11:15 10:11:20 10:11:23

So I went in -- in the green area, I'm actually searching on badguy.com, and with Encrypted Traffic Analytics turned on, if you look at the bottom blue portion to the right, you can actually see that we can see the domain name badguy.com. 10:11:28 10:11:31 10:11:36 10:11:40 10:11:45

So this is showing that with Encrypted Traffic Analytics turned on, utilizing the unencrypted components, I can actually determine threats within encrypted traffic and be able to have visibility into the domain name. 10:11:46 10:11:50 10:11:54 10:11:59

Q. Badguy.com is a known site that you're aware of that you've tested before? 10:12:03 10:12:08

A. Yes, it is. There's a lot of different bad sites out there, so that's one of the common sites that we use for testing and performing our analysis. 10:12:09 10:12:12 10:12:15

Q. So if we go to the next testing result, what happens when you turn ETA, or Encrypted Traffic Analytics, off, the switch, the Catalyst switch? 10:12:17 10:12:22 10:12:26

A. So when I turn Encrypted Traffic Analytics off and now I try to search for domain names or look for threats within the encrypted traffic without decrypting it, I now have no visibility. So now when I take that same stream of traffic 10:12:28 10:12:34 10:12:38 10:12:43

with Encrypted Traffic Analytics turned off and I search for badguy.com, I have no visibility. I have no visibility to what's happening, so this test shows that with Encrypted Traffic Analytics I have visibility into threats without decrypting the traffic, and I can utilize information such as domain names. 10:12:47 10:12:51 10:12:57 10:12:59 10:13:01 10:13:04

Q. Now let's talk about the '856 patent. 10:13:06

Could we show the animation we had at the beginning of the case, generally describing how the '856 patent works. 10:13:19 10:13:22

And, if you could, walk the Court through it just very briefly. 10:13:26 10:13:29

A. Sure. So with the '856 patent, you have your routers and switches analyzing encrypted and unencrypted traffic. The unencrypted has no lock, and the encrypted has a lock on it. And what it's able to do is first determine whether it's encrypted or unencrypted, and then it's able to utilize the unencrypted information to determine if there's threats in the encrypted traffic, utilizing information such as the domain name that I just showed you in the previous testing, and, based on that unencrypted information, it can determine if there's threats within the encrypted traffic. And then, based on that, it's able to then communicate and send rules to a proxy system, to be able to take action on the threats in the encrypted traffic. 10:13:30 10:13:34 10:13:41 10:13:45 10:13:49 10:13:54 10:13:57 10:14:00 10:14:03 10:14:07 10:14:12 10:14:17 10:14:21

Q. So if you go back to your testing of the badguys.com 10:14:23

website, if you saw that that encrypted traffic was from badguys.com, could you reroute it to a proxy system? 10:14:27 10:14:33

A. Exactly. That's an example of what the system would do. I manually did it with the testing, but that's exactly what the system would do. It would identify, via a threat feed, that badguy.com was bad. It would use unencrypted components of the encrypted traffic to identify badguy.com, recognize that's a threat, and then take that encrypted traffic and route it to a proxy. 10:14:36 10:14:41 10:14:44 10:14:48 10:14:53 10:14:55 10:14:59

Q. Now, let's take a look at how Cisco sets up its systems. 10:15:01

I'd like to show you what's been marked as PTX-989. Dr. Cole, do you know what this document is? 10:15:07 10:15:17

A. Yes. This is an internal document from Cisco Encrypted Traffic Analytics of February 2018, and this is an example of one of the many pieces of internal documents I utilized in order to draw my conclusions. 10:15:19 10:15:28 10:15:31 10:15:37

Q. And is this the Encrypted Traffic Analytics on the Catalyst 9000 switches, as shown on the title? 10:15:38 10:15:41

A. That is correct. 10:15:45

Q. If we turn to Page -- 10:15:46

MR. ANDRE: Your Honor, I'd like to move PTX-989 into evidence. 10:15:49 10:15:53

THE COURT: All right. This is the use of ETA on switches; is that correct? 10:15:59 10:16:03

MR. ANDRE: Dr. Cole? 10:16:10

THE WITNESS: Yes, that's correct. And what's important to point out is the infringing component that we're referring to, the ETA component that sits on routers and switches, is the same in both cases. So we're using a switch example, but the same components and same software reside on the router. So even though they're two different devices, they're using the same components on both. 10:16:11 10:16:13 10:16:19 10:16:22 10:16:27 10:16:31 10:16:35

THE COURT: When you say "the same components," would that be the same as saying "the same operating system"? 10:16:39 10:16:42

THE WITNESS: Yes. In this case, if you'll remember, there's the IOS, the Internet working operating system, and that resides on both of those systems, the routers and the switch, and the ETA software integrates with both of those. 10:16:49 10:16:52 10:16:55 10:17:00 10:17:04

I don't know if you're a car enthusiast, but the example would be you have the Chevy Corvette and the Camaro, but they both have the same engine. So if we were saying that the engine infringes, we could use either example, because it's the same engine in both cars. 10:17:05 10:17:08 10:17:13 10:17:17 10:17:21

THE COURT: I am a car enthusiast. 10:17:24

THE WITNESS: Excellent. We'd get along very well, then. 10:17:28 10:17:30

THE COURT: All right. Go ahead. 10:17:32

MR. ANDRE: Your Honor, is PTX-989 admitted? 10:17:34

THE COURT: Yes. 10:17:38

(Plaintiff's Exhibit PTX-989 was received in evidence.) 10:17:38 10:17:38

MR. ANDRE: Okay. Thank you. 10:17:38

BY MR. ANDRE: 10:17:38

Q. If we turn to Page 33 of this document, ending in Bates numbers 033, there's a diagram at the top that shows how Cisco -- it's the flow of their system when they're using the Catalyst switches. 10:17:40 10:17:44 10:17:52 10:18:01

Could you walk us through this flow diagram. 10:18:02

A. Yes. So if we start in the bottom, where it says "Catalyst 9000," this is the infringing Catalyst, but, as I said, the same IOS and ETA components reside on the router. So the router or switches, either one of those, could be in that bottom box. 10:18:05 10:18:07 10:18:14 10:18:20 10:18:22

They go in, and they look at the traffic, and they determine if it's encrypted or unencrypted, and then they send information up to Stealthwatch, and Stealthwatch is running your Encrypted Traffic Analytics and your Cognitive Threat Analytics, or CTA, and it analyzes that information to be able to identify threats in the encrypted traffic without decrypting it, and then it sends that information, utilizing the platform xGrid to the identity service engine, and then the identity service engine takes that information and sends it to the Catalyst switch, in this case, or the router and tells it to send it to a proxy, which in this case is going 10:18:23 10:18:26 10:18:31 10:18:37 10:18:41 10:18:47 10:18:52 10:18:57 10:19:02 10:19:07 10:19:11

to be the null interface that we're going to talk about later in the system -- later in my discussion. 10:19:15 10:19:19

So this lays out the entire infringing components. So you have the switches and routers, which determines encrypted/unencrypted, you have the Stealthwatch, that goes in and analyzes the unencrypted portions to determine threats in the encrypted, and then you have the identity service engine that's used as a communication path in order to proxy the traffic that has threats in the encrypted communication. 10:19:22 10:19:25 10:19:29 10:19:32 10:19:37 10:19:40 10:19:43

Q. In the upper right-hand corner there's something called Threat Grid. Is that the threat intelligence from other sources that are coming into the system? 10:19:48 10:19:51 10:19:54

A. Yes, that is the -- an example of the third-party threat information and threat analytics. When we get into the specific components of the claim, we will show that one example of that is Talos, that sends that threat information. But, yes, that's an example of the threat information. 10:19:55 10:20:02 10:20:06 10:20:09 10:20:13

Q. Let's go back and take the animation we showed earlier and plug this system into it, and, if you would, just walk through that very quickly, as you just did. 10:20:17 10:20:21 10:20:24

A. So you have your encrypted and unencrypted traffic going across the network. You have your accused routers or switches, which both are running the same internet-working operating system with Encrypted Traffic Analytics embedded into that, and they're able to determine whether there is 10:20:28 10:20:33 10:20:37 10:20:41 10:20:45

encrypted or unencrypted traffic. It sends that information up to Stealthwatch, that's running both Cognitive Threat Analytics, CTA, and Encrypted Traffic Analytics, ETA, and it's able to determine whether there's threats based on information it's getting from a third-party source -- you can see the cyber threat intelligence on the right-hand side feeding in -- and it's able to use that information in the unencrypted traffic to determine if there's threats in the encrypted traffic without decrypting it. It then sends that information to ISE, the Identity Service Engine, which then sends the rules to the routers and switches, which then has it proxy that information to a null interface. 10:20:49 10:20:52 10:20:56 10:21:01 10:21:05 10:21:07 10:21:11 10:21:15 10:21:18 10:21:23 10:21:28 10:21:33

Q. Thank you. Let's get -- 10:21:38

THE COURT: Can they obtain threat intelligence from any source other than Stealthwatch? 10:21:40 10:21:54

THE WITNESS: So Stealthwatch is the component that does the analytics, and it can receive third-party threat intelligence, so Stealthwatch can receive the threat intelligence from different sources. 10:21:56 10:22:05 10:22:08 10:22:12

One of the sources we're going to show when I show infringement is from Talos, but it can actually receive that threat intelligence from multiple sources. 10:22:14 10:22:18 10:22:22

MR. ANDRE: May I proceed, Your Honor? 10:22:31

THE COURT: But Stealthwatch is the component that receives the threat intelligence and introduces it to the 10:22:35 10:22:41

system? 10:22:46

THE WITNESS: Yes, exactly. Stealthwatch is the component that receives the threat intelligence to be able to do the analysis, yes. 10:22:48 10:22:50 10:22:54

THE COURT: All right. 10:22:57

BY MR. ANDRE: 10:22:58

Q. Dr. Cole, when you -- you can take that slide down. 10:23:00

When you were doing your analysis, did you use the claim construction that the Court provided in this case? 10:23:04 10:23:07

A. Yes, I did. 10:23:10

Q. And did you also use the claim construction that the parties agreed to in this case? 10:23:12 10:23:14

A. Yes, I did. 10:23:16

Q. Let's turn to claims 24 and 25 of the '856 patent. Let's start walking through it. 10:23:17 10:23:24

Could you describe the first element we're going to be discussing up in claim 24 and 25. 10:23:27 10:23:31

A. Yes. So claim 24, on the left-hand side, is a system claim, and claim 25, on the right-hand side, is a computer-readable media claim. So other than the preambles, which are slightly different, the remaining elements are very, very similar. 10:23:34 10:23:41 10:23:47 10:23:54 10:23:58

So we're going to start off by looking at the introductory components. So with claim 24 you need to have a hardware processor, and on claim 25 you need to have 10:23:59 10:24:02 10:24:07

computer-readable media that comprises instructions. 10:24:10

MR. ANDRE: We've gone over this with Dr. Mitzenmacher, but we'll go over this just very briefly, just to make sure that we have the evidence in, if Your Honor would like us to do so. We can do it very quickly. I don't want to repeat a lot of evidence, but, that being said, I think we'll take Your Honor's lead on this one. 10:24:17 10:24:19 10:24:22 10:24:26 10:24:28 10:24:32

THE COURT: Well, I'm not going to tell you how to proceed. 10:24:35 10:24:42

MR. ANDRE: Okay. I'll go through it very quickly, then. 10:24:42 10:24:43

BY MR. ANDRE: 10:24:44

Q. Dr. Cole, let me show you what's been marked as PTX-524. 10:24:44

MR. ANDRE: This has already been admitted into evidence. 10:24:49 10:24:52

BY MR. ANDRE: 10:24:52

Q. What is this document, Dr. Cole? 10:24:53

A. This is the Cisco 4000 series integrated services router specification sheet that shows the specifications for these computing devices. 10:24:55 10:25:04 10:25:07

Q. If we go to Page 3 of this document, there's a table there. 10:25:09 10:25:13

Could you describe how the -- the top part, originally, how that influenced your opinion as to whether or not the routers have a processor. 10:25:13 10:25:21 10:25:24

A. As I mentioned, these are physical devices, and they have processors, memory, hard drives, storage, Ethernet cards, just like a regular computer does, and when we're looking at the architectural highlights, you can see that it has a multicore processor, and it even talks about the high-performance multicore processor. 10:25:31 10:25:35 10:25:40 10:25:43 10:25:46 10:25:50

So this supports, just as Dr. Mitzenmacher went over yesterday, that these are physical boxes with processors, memory, and hard drives. 10:25:52 10:25:57 10:26:00

Q. If we go to the bottom of that chart, where it says, "Flash Memory Support and DRAM," could you describe how that supports your opinion that these systems have a processor and memory and computer-readable media. 10:26:02 10:26:06 10:26:11 10:26:14

A. So when we look at the memory support, you can see that it supports flash memory, upgradable up to 32 gigabytes. That's what GB, gigabytes, is. 10:26:19 10:26:23 10:26:28

Then with DRAM, that is dynamic random access memory, and you can see that it also has up to 4 gigabytes of fixed dynamic random access memory. 10:26:31 10:26:37 10:26:42

Q. Okay. Let's go to PTX-573. 10:26:45

MR. ANDRE: This is the ASR routers, and, Your Honor, this has not been admitted into evidence. 10:26:55 10:26:58

May we -- 10:26:58

BY MR. ANDRE: 10:26:58

Q. First of all, Dr. Cole, what is PTX-573? 10:27:04

A. This is the document for the Cisco ASR 1000 series route processors. 10:27:08 10:27:13

So we're going through the different infringing routers and switches to show that they all have processors, memory, and computer-readable medium, but they all operate in the same fashion, so we're trying to go through this quickly to show you the supporting evidence. 10:27:15 10:27:17 10:27:23 10:27:27 10:27:30

Q. If you go to the table at the bottom of the first page -- 10:27:33

MR. ANDRE: Your Honor, I'd like to move PTX-573 into evidence. 10:27:33 10:27:36

THE COURT: That will be admitted. 10:27:37

Was 524 previously admitted? 10:27:38

MR. ANDRE: It was, Your Honor. It was with Dr. Mitzenmacher. 10:27:40 10:27:43

THE COURT: Okay. 10:27:46

(Plaintiff's Exhibit PTX-573 was received in evidence.) 10:27:46 10:27:47

BY MR. ANDRE: 10:27:47

Q. And could you pull up the whole table at the bottom of the page? 10:27:49 10:27:54

THE COURT: Are we looking at 573? 10:27:54

MR. ANDRE: Yes, that's correct, Your Honor, Page 1. 10:27:58

THE COURT: Okay. 10:28:00

THE WITNESS: So this is showing the actual route processors, and you can actually see pictures. These are 10:28:06 10:28:09

physical computing devices. 10:28:12

And if we go in and look under CPU, that stands for central processing unit, so that's the processor on the system. And depending on which type of router, you can have a general purpose central processing unit, you can have dual core -- that means two -- processors, you can have quad core, four processors. So this fully supports that there are processors. 10:28:15 10:28:19 10:28:23 10:28:28 10:28:33 10:28:39 10:28:41

And then if we go under memory, you can see that they have 4 gigabytes for the RP1, 8 gigabytes or 16 gigabytes for RP2. And this is a great chart, because it really shows you the difference between all the routers and switches. They're all computing devices, it's just they have different numbers of processors and different amounts of memory. But they all have memory, and they all have processors, and if we actually go to the next page, you can actually see where it actually loads the code, the computer-readable media, onto the memory. 10:28:42 10:28:46 10:28:53 10:28:57 10:29:00 10:29:03 10:29:07 10:29:10 10:29:14 10:29:17

BY MR. ANDRE: 10:29:30

Q. Geoff, can you go to the next page? 10:29:31

A. And if you look at the third bullet, it says, "the hard disc drive or solid state drive for code storage." So it actually supports the computer-readable media; that there's actually code that's stored on the hard drive on these physical devices that have processors and memory. 10:29:33 10:29:36 10:29:41 10:29:44 10:29:47

Q. And if we go to PTX-1008, Dr. Cole, what is PTX-1008? 10:29:54
A. This is a Cisco document on the Cisco Catalyst 9300 series switches. 10:30:04 10:30:12
MR. ANDRE: Your Honor, I'd like to move in PTX-1008. 10:30:15 10:30:19
MR. JAMESON: No objection. 10:30:27
THE COURT: PTX-1008 will be admitted. 10:30:28
(Plaintiff's Exhibit PTX-1008 was received in evidence.) 10:30:32 10:30:34
BY MR. ANDRE: 10:30:34
Q. Dr. Cole, if we go to Page 4 of this document ending in Bates number 004 and put in the first several bullet points under "Product Overview and Features," could you describe to the Court how this informs your opinion as to whether or not the Catalyst switches have the processor, memory, and computer-readable media. 10:30:34 10:30:37 10:30:43 10:30:49 10:30:52 10:30:56
A. Yes. So, specifically, if we look at the third bullet, CPU is central processing unit. So this is showing that there's a processor on the system. 10:30:59 10:31:03 10:31:08
It also shows that there is 8 gigabytes of memory and 16 gigabytes of external storage. 10:31:11 10:31:15
You also have SSD, solid state drive, and this is the hard drive that actually stores the code that every time you are running, the device actually loads that computer-readable medium off the hard drive to actually allow 10:31:21 10:31:25 10:31:29 10:31:33

the system to function and run correctly. 10:31:37
Q. Let's go back to the claim slide again. 10:31:42
Dr. Cole, based on the evidence that you've 10:31:46
discussed here today and that's been introduced in this case, 10:31:48
did you form an opinion as to whether or not the accused 10:31:52
Catalyst switches and the routers in this case, the ISR and 10:31:57
ASR routers, meet the first claimed element of claims 24 and 10:32:03
25? 10:32:08
A. Yes. I looked at a large amount of evidence. We showed 10:32:08
a sampling of it, but it clearly shows that there's hardware 10:32:12
processors and memory-storing instructions for claim 24, and 10:32:15
it clearly shows that there's computer-readable medium 10:32:18
comprising instructions stored on the hard drive and the 10:32:22
hardware processors, so it meets the elements of claim 25. 10:32:25
So we can definitely check those boxes. 10:32:28
Q. All right. Let's turn our attention to the second 10:32:33
element: "Receive data indicating a plurality of network 10:32:35
threat indicators." 10:32:42
Can you describe what you're looking for in this 10:32:44
element? 10:32:46
A. In this element I'm looking for two main things. One is 10:32:46
that -- in this case, it's going to be Stealthwatch is 10:32:48
receiving network threat indicators and that at least one of 10:32:52
those network threat indicators contains a domain name. And 10:32:56
we sort of foreshadowed this when we went in and showed you 10:33:03

the testing I did with Wireshark. We were actually able to see the domain name within that traffic. 10:33:07 10:33:10

Q. And is this the identical element for claims 24 and 25? 10:33:11

A. Yes. For the next several claims, the language is going to be identical for both 24 and 25, so we're going to do those together. 10:33:19 10:33:23 10:33:27

Q. All right. Let's do -- let's first turn our attention to PTX-20. 10:33:28 10:33:33

Dr. Cole, what is this document? 10:33:40

A. This is a Cisco document talking about Cisco Stealthwatch Enterprise, and, as I mentioned, Stealthwatch is the component that's going to be receiving the threat intelligence. 10:33:41 10:33:49 10:33:53 10:33:56

Q. And if we -- 10:33:56

MR. ANDRE: Your Honor, I'd like to move PTX-20 into evidence. 10:33:59 10:34:02

MR. JAMESON: No objection. 10:34:03

THE COURT: PTX-20 will be admitted. 10:34:04

(Plaintiff's Exhibit PTX-20 was received in evidence.) 10:34:04 10:10:20

BY MR. ANDRE: 10:34:07

Q. And, Dr. Cole, if you look at the first paragraph of this document, could you look at that and tell the Court how this informed your opinion as to the second claim element of receiving threat indicators. 10:34:08 10:34:09 10:34:13 10:34:18

A. Yes. This talks about Stealthwatch Enterprise; that it performs security analytics and it leverages enterprise telemetry from the existing network infrastructure. So that's showing as receiving threat intelligence. It provides advanced threat detection, accelerated response, and simplified segmentation using a multilayer machine learning and advanced behavioral modeling across the network. And it also shows you, in the second paragraph, that Stealthwatch Enterprise gets you real-time visibility into activities occurring within the network. 10:34:23 10:34:28 10:34:33 10:34:37 10:34:42 10:34:45 10:34:51 10:34:54 10:34:57 10:35:02

Q. And is that your opinion, that the system receives data indicating a plurality of network threat indicators? 10:35:03 10:35:12

A. Yes, it does. And in the bullets below this paragraph, it actually further supports that it receives the threat information and the threat indicators. So, yes, this is one of many documents that supports that. 10:35:16 10:35:21 10:35:23 10:35:26

So if we look under "System Benefits," you can see real-time threat detection, incident response, network performance. Once again, this all supports that Stealthwatch receives third-party threat indicators. 10:35:28 10:35:34 10:35:39 10:35:42

Q. If we go to the second page of this document, at the top there's a paragraph entitled "Flow Collector." 10:35:46 10:35:49

Could you describe to the Court how this influenced your opinion regarding the second claim element, receiving data indicating a plurality of threat indicators. 10:35:52 10:35:56 10:36:00

A. Yeah. So it shows a flow collector, which is a component of Stealthwatch, leverages enterprise telemetry, such as NetFlow, IPFIX, and other types of data flow, from existing infrastructure, such as routers, switches, and firewalls. 10:36:04 10:36:08 10:36:13 10:36:21

And then it goes on to say that the flow collector can also receive and collect telemetry from proxy data sources, which can be analyzed by the global threat analytics. So this is also showing that it can receive, get, gather, information on threat indicators from third parties. 10:36:25 10:36:27 10:36:32 10:36:37 10:36:40

Q. And then how does ETA, Encrypted Traffic Analytics -- how is that utilized in this flow collection? 10:36:45 10:36:55

A. Encrypted Traffic Analytics is a key part of Stealthwatch, so it says, "Stealthwatch Enterprise, using the Encrypted Traffic Analytics, can use analytics to pinpoint malicious patterns in encrypted traffic to identify threats and accelerate response and, through this feature, is built into the system at no extra cost." 10:36:58 10:37:03 10:37:08 10:37:11 10:37:16 10:37:20

So this is showing that this ETA is able to use those indicators to analyze the encrypted traffic to find threats within the encrypted traffic without actually decrypting it. 10:37:24 10:37:28 10:37:33 10:37:35

Q. Let me show you what's been marked as PTX-1018 -- sorry, 1081. I inverted. 10:37:36 10:37:52

MR. ANDRE: Sorry, Your Honor. 10:38:04

BY MR. ANDRE: 10:38:06

Q. Dr. Cole, what is PTX-1081? 10:38:06
A. This is a Cisco presentation talking about combining 10:38:09
cognitive analytics with Stealthwatch for malware detection. 10:38:13
And, once again, it's important to point out the date of this 10:38:16
document is June 2017. 10:38:20
MR. ANDRE: Your Honor, I'd like to move Exhibit 10:38:23
PTX-1081 into evidence. 10:38:25
THE COURT: That will be admitted. 10:38:36
(Plaintiff's Exhibit PTX-1081 was received in 10:38:37
evidence.) 10:38:38
BY MR. ANDRE: 10:38:38
Q. Dr. Cole, I'd like to turn your attention to Page 13 of 10:38:40
this document ending in Bates number 013. 10:38:44
Could you tell the Court how this informs your 10:38:51
opinion as to whether or not one of the plurality of network 10:38:54
indicators comprises a domain name. 10:38:59
A. So this is the global risk map, and this draws in all the 10:39:02
different threat information into Stealthwatch. And it shows 10:39:07
you that it has many features, but if we look at that third 10:39:12
bullet, one of the features is that it includes domain data, 10:39:16
which is another way of specifying domain names, and an 10:39:21
example of domain name is what we saw earlier with my 10:39:26
testing, which is badguy.com. So this shows that -- 10:39:30
THE COURT: I'm sorry. What exhibit is this? I 10:39:33
lost the number. 10:39:37

MR. ANDRE: This is 1081, Your Honor, on Page 13. 10:39:38

THE COURT: All right, I've got it. Continue. 10:40:00

BY MR. ANDRE: 10:40:03

Q. Dr. Cole, what were you saying about how this shows the 10:40:07
domain data? 10:40:11

A. Yes. So this is the global risk map, and this shows that 10:40:12
Stealthwatch is pulling in information from different 10:40:16
sources. 10:40:19

So you can see in that first bullet they use up to 10:40:20
20 features of 150 million of malicious or risky information, 10:40:24
so that's pulling in the threat indicators. 10:40:29

And then it shows in the third bullet that it can 10:40:32
include domain data, which is another way of specifying 10:40:35
domain names. And an example of a domain name would be 10:40:40
badguy.com, that we previously looked at during my testing. 10:40:43

Q. Dr. Cole, I'd like to look at one more exhibit, PTX-1010. 10:40:48

Could you inform the Court what this document is? 10:40:59

A. This is a Cisco public document on Cisco Stealthwatch 10:41:01
threat intelligence license where it talks about the Cisco 10:41:08
Stealthwatch threat intelligence and the licensing and the 10:41:12
details behind it. 10:41:14

MR. ANDRE: Your Honor, I'd like to move PTX-1010 10:41:16
into evidence. 10:41:19

THE COURT: That will be admitted. 10:41:19

(Plaintiff's Exhibit PTX-1010 was received in 10:41:19

evidence.)

BY MR. ANDRE:

Q. And, Dr. Cole, I want to turn your attention to the first page of this document. On the left-hand side, there's a figure and a paragraph above that.

Could you describe what is being discussed and what is being shown in that figure and how it relates to your opinion that the system receives data indicating a plurality of network threat indicators.

THE COURT: What page is this?

MR. ANDRE: This is the first page, Your Honor, on the left-hand side, the bottom left corner.

THE COURT: Okay.

THE WITNESS: So, essentially, the text on the top is describing what is in the diagram below, so I'll cover these simultaneously.

So in the diagram, on the left-hand side is Stealthwatch, and then on the right-hand side is the global threat intelligence feed that, as I mentioned earlier in my testimony, is powered by Talos. And, as you can see, this is a global threat intelligence network, where you're getting all this information from all these different platforms, and it's all being fed into Stealthwatch.

So all the information on the right in the globe is actually being moved into Stealthwatch, and that's where it's

receiving that threat intelligence. And, as we saw previously, that threat intelligence contains many pieces of information, including a domain name. 10:42:41 10:42:43 10:42:47

BY MR. ANDRE: 10:42:49

Q. Now, I want to show you a piece of testimony from a Cisco principal engineer, Mr. Amin. This is PTX-1926. 10:42:52 10:42:55

MR. ANDRE: And, Your Honor, I'd like to admit PTX-1926 into evidence. This was played last Friday in open court. 10:43:01 10:43:03 10:43:07

THE COURT: Was it admitted at that time? 10:43:10

MR. ANDRE: This slide was not, but the deposition was played, the entire clip was. 10:43:13 10:43:16

THE COURT: All right. What's the PTX number? 10:43:26

MR. ANDRE: 1926. 10:43:27

THE COURT: And this is a slide? 10:43:31

MR. ANDRE: It is, Your Honor. 10:43:35

THE COURT: All right. 10:43:36

(Plaintiff's Exhibit PTX-1926 was received in evidence.) 10:43:36 10:10:20

BY MR. ANDRE: 10:43:37

Q. Dr. Cole, could you explain how Mr. Amin's deposition testimony informed your opinion regarding the use of domain names as a threat indicator? 10:43:38 10:43:43 10:43:46

A. Yes. So starting at the top, he's asked, "Does Stealthwatch receive threat intelligence in a particular 10:43:50 10:43:53

format?" And the answer is, "The Stealthwatch system receives threat intelligence in a particular format, yes." So this shows that Stealthwatch receives threat intelligence. 10:43:56 10:44:00 10:44:03

He then goes on to talk about the formatting, and the second important piece is at the very bottom, where when he's asked, "What is contained in this file," he says, "A list of IP addresses and domain names." 10:44:08 10:44:13 10:44:16 10:44:21

So this shows me from Cisco's own principal engineer that not only Stealthwatch receives threat intelligence, but that threat intelligence contains a domain name. 10:44:25 10:44:29 10:44:32

Q. If we could go back to the claim slide, based on all of the information you reviewed in this case, the exhibits you identified to the Court today, the testing, and the testimony you've seen, did you form an opinion as to whether or not the accused Cisco system that you discussed here today -- the Catalyst switches, the ASR/ISR routers, Stealthwatch, and the Identity Services Engine -- infringe the second element of claims 24 and 25? 10:44:38 10:44:45 10:44:49 10:44:53 10:44:56 10:45:00 10:45:04 10:45:08

A. Yes. We clearly saw that it receives a plurality of network threat indicators and, through both documents and testimony and testing, that it comprises a domain name identified as a network threat. 10:45:09 10:45:16 10:45:20 10:45:23

Q. Let's turn our -- actually, the next two elements we're going to take together. 10:45:25 10:45:30

A. Can I actually check the box? 10:45:32

Q. Sorry. I don't want to deprive you of checking the box. Check the box, yes. 10:45:35 10:45:39

A. Yes, we can check the box. 10:45:40

Q. You do a lot of work to check those boxes. I understand. Sorry to skip it. 10:45:42 10:45:45

All right. Dr. Cole, is it okay -- these next two elements, could you describe what they're discussing and why we're taking them together? 10:45:47 10:45:49 10:45:52

A. Yes. So the next two elements -- the first one is identifying packets comprising unencrypted data, and the second one is identifying packets comprising encrypted data. 10:45:53 10:45:58 10:46:03

The reason we're taking these together is the Encrypted Traffic Analytics component on the switch and the routers -- it goes in, and it looks at the traffic and says, is this encrypted? So if it comes back and says, no, then it identified unencrypted data, and if it comes back and says, yes, then it identified encrypted data. 10:46:07 10:46:10 10:46:13 10:46:19 10:46:25 10:46:29

So it's the same component that's looking at that traffic that's going to determine either it's unencrypted or encrypted. So because it's the same component, it made sense to cover these together. 10:46:32 10:46:35 10:46:38 10:46:41

Q. Okay. Let's turn our attention to PTX-989. 10:46:43

MR. ANDRE: Which we saw earlier today, Your Honor. It's been admitted. 10:46:50 10:46:52

BY MR. ANDRE: 10:46:52

Q. We're going to turn to Page 4, ending in Bates number 004. 10:46:54 10:47:01

A. Yes. I just want to highlight that even though this document is for the 9000 switch, Catalyst switch, the same functionality, the same ETA and IOS, is on the routers, also. So this same component applies to both switches and routers. 10:47:05 10:47:07 10:47:14 10:47:19

And then in this slide we're seeing that it can go in and be able to determine whether it's encrypted or unencrypted traffic. And if we actually look at the text that goes along with this slide, it says, "We've enhanced the network as a sensor to detect malicious patterns in not only encrypted [sic] traffic but also in encrypted traffic." 10:47:25 10:47:27 10:47:33 10:47:39 10:47:45 10:47:50

So this clearly shows, both with the wording and with the diagram, and I've confirmed it with my other analysis and testing, that the infringing components can go in and identify both encrypted and unencrypted traffic. 10:47:54 10:47:57 10:48:03 10:48:06

Q. I'd like to turn your attention to PTX-570. 10:48:08

Dr. Cole, what is PTX-570? 10:48:19

A. This is a Cisco document, Encrypted Traffic Analytics Deployment Guide, from July 2019. 10:48:21 10:48:27

MR. ANDRE: And, Your Honor, I'd like to move PTX-570 into evidence. 10:48:33 10:48:36

THE COURT: PTX-570 will be admitted. 10:48:39

(Plaintiff's Exhibit PTX-570 was received in evidence.) 10:48:44 10:48:45

BY MR. ANDRE: 10:48:45

Q. Dr. Cole, would you please turn to -- first of all, what is the date of this document? 10:48:48 10:48:53

A. The date of the document is July 2019. 10:48:54

Q. If we turn to what is Page 11 of the document -- it's Bates numbers 9600 -- if we look at that first paragraph under "Solution," could you describe -- first of all, which switches and which routers are we talking about here? 10:48:58 10:49:05 10:49:15 10:49:20

A. The switches and routers that are listed in the first sentence, this is a list of the infringing routers and switches. So if we go back to yesterday where we talked about all the switches and routers that are infringing, this is a list that specifies all of those. 10:49:23 10:49:29 10:49:34 10:49:38 10:49:40

Q. And if you look at the second line, the routers are running the Cisco IOS XE 16.6.4. Do you see that? 10:49:43 10:49:49

A. Yes, I do. 10:49:55

Q. Now, if you look down to where it talks about using -- how it monitors encrypted data, can you inform the Court how this informs your opinion as to the identification of unencrypted and encrypted data. 10:49:56 10:50:05 10:50:12 10:50:13

A. So if we continue at the end of the second line into the third line, you can enable Encrypted Traffic Analytics, in addition to flexible NetFlow on switch or routers -- so it shows it's the same component on both the switches and the routers -- and passively monitor encrypted flows. 10:50:17 10:50:21 10:50:26 10:50:30 10:50:33

So if you're monitoring the encrypted flows, then you're also able to determine whether it's unencrypted on the system. So this is showing that it can identify both encrypted and unencrypted traffic. And then it also goes in and will foreshadow some of the claims we'll cover in a little bit, where it talks about the unencrypted metadata can be used to collect information regarding the cipher suite version and clients' public key length as reported by the cipher suite. So it shows that it uses the unencrypted portion to be able to identify threats in the encrypted traffic. 10:50:37 10:50:40 10:50:44 10:50:48 10:50:53 10:50:58 10:51:02 10:51:07 10:51:12 10:51:15 10:51:17

Q. So when we get to that claim element regarding using the unencrypted portion to determine the encrypted portion in later elements, we can refer back to this exhibit, PTX-570? 10:51:18 10:51:21 10:51:23

A. Yes, we can. 10:51:28

Q. Okay. And I'd like to show you what's been marked as PTX-578. 10:51:30 10:51:32

Dr. Cole, what is this document? 10:51:39

A. This is a Cisco presentation on encrypting threat analytics, which we've been referring to as ETA. And even in the title it confirms detecting malware without encryption, and this is from one of the principal engineers, and this document is from July 20th, 2018. 10:51:40 10:51:48 10:51:53 10:51:58 10:52:02

MR. ANDRE: Your Honor, I'd like to move in PTX-578 into evidence. 10:52:06 10:52:10

THE COURT: That will be admitted. 10:52:13

(Plaintiff's Exhibit PTX-578 was received in evidence.) 10:52:14 10:52:16

BY MR. ANDRE: 10:52:16

Q. And, Dr. Cole, if we could turn to Page 11 of this document ending in Bates number 061, could you describe to the Court how this figure informs your opinion as to how Cisco uses encrypted -- identifies encrypted and unencrypted packets. 10:52:17 10:52:20 10:52:26 10:52:33 10:52:42

A. So this is the process flow that's similar to the previous document, not only proves this element but also proves the future elements, but it shows how can we inspect encrypted traffic. And it goes in and it does an initial data packet analysis, where it goes in and it looks at the fields to determine whether this is encrypted or unencrypted, and it's using unencrypted fields, such as sequence of packet length and time, to identify different content, and then it's utilizing the global risk map on the Who's Who of the internet to do that analysis. 10:52:43 10:52:48 10:52:52 10:52:56 10:52:59 10:53:03 10:53:07 10:53:12 10:53:16 10:53:21

So the right-hand side, the global risk map, further supports the previous element that it's receiving threat intelligence that contains domain names, and then the left-hand side shows that it's able to determine encrypted and unencrypted traffic. 10:53:23 10:53:26 10:53:30 10:53:33 10:53:37

Q. All right. 10:53:39

MR. ANDRE: And, Your Honor, at this point I want to show Dr. Cole one piece of source code, so I'd like to seal the courtroom for about three minutes. 10:53:42 10:53:44 10:53:47

THE COURT: All right. 10:53:49

MR. ANDRE: Mr. Jonathan Rogers will step out of the room for five minutes. He's confirmed that. 10:53:58 10:54:02

(Confidential testimony from Page 933, Line 7, through Page 934, Line 20, was redacted.)

* * * * * * *

(Confidential testimony from Page 933, Line 7, through Page 934, Line 20, was redacted.)

* * * * * * *

BY MR. ANDRE:

Q. And, Dr. Cole, going back to the checkbox, based on the information you provided here today, the testing you did and the exhibits you reviewed, did you form an opinion as to whether or not the accused Cisco systems infringed the

10:56:22
10:56:22
10:56:22
10:56:27
10:56:32
10:56:34

identifying the packets comprising unencrypted data and identifying the packets comprising the encrypted data claim elements? 10:56:39 10:56:42 10:56:47

A. Yes, clearly. Based on all the analysis that I did and a sampling of the evidence that we showed today, it clearly identifies both encrypted data and unencrypted data, so we can check both of those boxes. 10:56:47 10:56:51 10:56:54 10:56:58

Q. All right. Let's go to the next element. 10:56:59

It's determined, based on the unencrypted data or a portion of unencrypted data, to one or more network threat indicators, packets comprising encrypted data correspond to the threat indicator. 10:57:05 10:57:08 10:57:11 10:57:17

You described -- you discussed this already some today, and we'll look back to those exhibits, but what are we looking at here? 10:57:18 10:57:20 10:57:22

A. Essentially, I know this is a longer claim element, but really what this is saying is being able to determine if there's threat indicators in encrypted traffic without decrypting it. Or another way of saying it is by utilizing unencrypted data, we can actually determine if there's threat indicators in the encrypted data without actually having to decrypt the data, and this allows it to get much faster analysis of those network threats. 10:57:22 10:57:28 10:57:33 10:57:38 10:57:43 10:57:49 10:57:52 10:57:58

Q. And you pointed to this element previously when you were showing the previous elements. 10:58:00 10:58:06

Did Exhibits PTX-570 and PTX-578 inform your opinion as to this element that you testified just previous to, just right before this element? 10:58:08 10:58:13 10:58:19

A. Yes. Both of them -- just to refresh the Court, both of them clearly stated that Encrypted Traffic Analytics allows threats in encrypted traffic to be detected without decrypting the data. And, also, both of those pieces of evidence also stated that by utilizing the unencrypted portion, we can identify threats in the encrypted portion without decrypting it. 10:58:20 10:58:24 10:58:30 10:58:36 10:58:40 10:58:44 10:58:48

THE COURT: Well, that's the header and the receipt. In other words, who is sending it and who is receiving it is what you look at to determine if it's a threat. 10:58:49 10:58:56 10:59:00

THE WITNESS: Correct, Your Honor. So the header information on who is sending and receiving is one piece of information, but the other piece of information that we saw in the previous slides is there's unencrypted information in the Transport Layer Security. That's the encrypted component handshake that's also utilized -- that's unencrypted that's also utilized to determine threats in the encrypted traffic. 10:59:05 10:59:10 10:59:15 10:59:19 10:59:24 10:59:29 10:59:33

THE COURT: Such as volume? 10:59:38

THE WITNESS: Exactly, such as volume, traffic flows, length, and other factors. 10:59:42 10:59:45

BY MR. ANDRE: 10:59:50

Q. And let's turn to that on PTX-989. 10:59:51

MR. ANDRE: Which has been admitted into evidence, Your Honor. 10:59:53 10:59:55

BY MR. ANDRE: 10:59:55

Q. If we go to Page 24 of this document, could you describe some of those factors that's being described here in this figure. 10:59:56 11:00:02 11:00:06

A. Yes. So this shows two of the components that cognitive analytics uses for malware detection. And this aligns exactly with what Your Honor just said; where, by utilizing sequence of packets, lengths, and times on the bottom, and the initial data packet of the Transport Layer Security header, it's able to utilize that unencrypted information to determine if there's threats in the encrypted traffic without decrypting it. 11:00:08 11:00:14 11:00:19 11:00:26 11:00:28 11:00:31 11:00:35 11:00:38

And this slide also further supports the previous claims where, in the upper right-hand side, you see that threat intelligence map, where those threats are coming in from third parties. 11:00:40 11:00:44 11:00:47 11:00:50

Q. Let me show you another document that we'll show what the initial data packet comprises. We'll go to PTX-1066. 11:00:53 11:00:58

THE COURT: This is a new exhibit? 11:01:04

MR. ANDRE: It is, Your Honor. 11:01:07

BY MR. ANDRE: 11:01:10

Q. Dr. Cole, what is Exhibit 1066? 11:01:10

A. This is a Cisco internal presentation on Encrypted 11:01:14

Traffic Analytics, where it's talking about the network telemetry and machine learning. 11:01:20 11:01:22

MR. ANDRE: Your Honor, I'd like to admit Exhibit 1066 into evidence. 11:01:26 11:01:30

THE COURT: Machine learning -- 11:01:41

MR. JAMESON: No objection, Your Honor. 11:01:51

THE COURT: When I hear "machine learning," it makes me think of the term "artificial intelligence." I'm not sure how that term fits into our analysis of the patents, since nobody can agree on what the term means, but that means that the machine learns, I suppose, through the introduction of new rules, where to look for threats. 11:02:02 11:02:05 11:02:11 11:02:23 11:02:29 11:02:36

THE WITNESS: Yes, Your Honor. Like you said, there's different definitions of "artificial intelligence." The way that I always used it when I was at the CIA and did programming is where you can have computers mimic human intelligence. And one way of doing that is by giving it large data sets of good traffic and bad traffic and have the machine actually learn what is good and what is bad. 11:02:45 11:02:47 11:02:50 11:02:55 11:02:59 11:03:04 11:03:07

I want to make sure I answered your question, but in terms of this patent, the machine learning component really doesn't come into play, so we're not going to actually be referring to those portions of this document. But I did want to answer your question. 11:03:12 11:03:15 11:03:18 11:03:21 11:03:24

THE COURT: Okay. 11:03:26

BY MR. ANDRE: 11:03:26

Q. Turn to Page 15 of this document ending in Bates 015. 11:03:30

Dr. Cole, could you describe what type of 11:03:35

unencrypted information is in the initial data packet. 11:03:38

A. Yes. So if we look at the right-hand side, the graphic, 11:03:41

you have your IP header, which is what's been referred to so 11:03:50

far in this trial as layer 3, and the TCP header as layer 4, 11:03:57

but then there's also the Transport Layer Security header, 11:04:05

which is the new version of Secure Socket Layer, which you 11:04:10

might have heard as SSL, and this shows us some of the 11:04:16

unencrypted information in the initial Transport Layer 11:04:21

Security header. 11:04:25

Just to back up for a second, Transport Layer 11:04:27

Security is the encrypted communication, but in order to set 11:04:30

up that encrypted communication, there has to be some initial 11:04:34

information, such as the version, the server name, and the 11:04:38

cipher suites that have to be exchanged, unencrypted, before 11:04:44

that happens. So this is also some initial unencrypted 11:04:48

information in that initial data packet that's actually used 11:04:52

to determine if there's threats in the encrypted traffic. 11:04:56

MR. ANDRE: Your Honor, I don't know if I've done 11:05:06

this. I do want to move in PTX-1066 into evidence. 11:05:07

THE COURT: That will be admitted. 11:05:11

(Plaintiff's Exhibit PTX-1066 was received in 11:05:13

evidence.) 11:05:14

MR. ANDRE: Thank you. 11:05:14

BY MR. ANDRE: 11:05:17

Q. Dr. Cole, I want to show you another exhibit, PTX-1009. 11:05:18

Can you describe to the Court what this document is? 11:05:32

A. Yes. This is release notes for Cognitive Intelligence, 11:05:34

or what they're saying was formerly Cognitive Threat 11:05:42

Analytics. 11:05:45

And what this is is whenever you put out new 11:05:46

products, they do release notes to tell people what the 11:05:49

product does and how the product operates and functions. 11:05:53

MR. ANDRE: Your Honor, I'd like to move in 11:05:57

PTX-1009. 11:06:01

THE COURT: That will be admitted. 11:06:01

(Plaintiff's Exhibit PTX-1009 was received in 11:06:04

evidence.) 11:06:04

BY MR. ANDRE: 11:06:04

Q. Doctor, would you turn to Page 12 of this document, 11:06:05

ending in Bates 012. There's a November 2017 heading with 11:06:07

"Encrypted Traffic Analytics." 11:06:13

Could you describe how that first couple bullet 11:06:16

points inform your opinion as to whether or not the system 11:06:22

uses the unencrypted data to make determinations on the 11:06:24

encrypted data. 11:06:28

A. Yeah. The first sentence clearly shows this, where it 11:06:30

says, "Encrypted Traffic Analytics enhances existing 11:06:33

Stealthwatch and CTA" -- which is Cognitive Threat Analytics -- "integration with malware detection capability for encrypted traffic without decryption." 11:06:37 11:06:41 11:06:45

So this further shows that it's able to analyze threats in the encrypted traffic without decrypting it, and, as we saw with the previous evidence, it does that by looking at unencrypted information, identifying threats, and uses that to identify threats in the encrypted portion. 11:06:50 11:06:53 11:06:57 11:07:01 11:07:06

Q. The second bullet point, talking about identifying malware in encrypted traffic is done through inference using multiple sources of data, what's that referring to? 11:07:12 11:07:14 11:07:18

A. This supports what was in the previous claim, where it says that it gets threat indicators from third-party sources. So this further supports that it's receiving that information, and then it goes on to show that there is no -- sorry -- there is no decryption or inspection of traffic contact, privacy is maintained at all times. 11:07:21 11:07:26 11:07:31 11:07:34 11:07:38 11:07:45

And the reason why that is so important is that was the problem that they had with the old method. The old method, before Centripetal invented the '856 patent, was you had to decrypt all the traffic, which created major privacy concerns. So if I was at work and I was checking my bank account or my medical record and the company was decrypting all that traffic, that would create privacy and regulation issues, and they could actually be at risk. So one of the 11:07:46 11:07:49 11:07:53 11:07:59 11:08:05 11:08:09 11:08:13 11:08:17

key components of the '856 invention is that the privacy is maintained at all times, because decryption doesn't occur of the traffic. 11:08:22 11:08:26 11:08:30

THE COURT: Well, the paper this morning was talking about two countries allegedly exfiltrating data from our pharmaceutical companies and universities to prevent us from developing a virus vaccine. Did anybody see that? 11:08:34 11:08:38 11:08:51 11:09:00

THE WITNESS: Yes, I did. I actually read that story. And, actually, I believe it was CBS -- I actually did a little news segment on that this morning. 11:09:08 11:09:11 11:09:16

THE COURT: Is that right? 11:09:16

THE WITNESS: I was up since 5:00 a.m., East Coast time. 11:09:20 11:09:27

THE COURT: Where are you? 11:09:27

THE WITNESS: I'm in Northern Virginia, so I'm on East Coast. That's a normal day for me. I normally get up at that time 4:00, 4:30 a.m., because I have to watch the news, and then I normally do interviews with the various news services, based on cyber security stories, before I start my day. 11:09:27 11:09:31 11:09:35 11:09:38 11:09:42 11:09:45

THE COURT: All right. 11:09:46

BY MR. ANDRE: 11:09:47

Q. And one last document I want to show you, Dr. Cole. 11:09:47

THE COURT: Well, let me understand something. 11:09:51

Are they being -- they're not -- is "exfiltrating" 11:09:54

the right word? I mean, they're removing the data so that it can't get to the recipient. Is that what they're doing, allegedly? 11:10:03 11:10:08 11:10:11

THE WITNESS: They're allegedly doing two things. 11:10:11

One is they're exfiltrating the data so they can actually develop a vaccine before the U.S. can, because, as you can imagine, a vaccine for COVID-19 is a billion-dollar vaccine. So they're trying to steal it, and then, because they're so clever, they're trying to alter the actual vaccine so it doesn't work so the U.S. can't produce. 11:10:14 11:10:20 11:10:24 11:10:32 11:10:35 11:10:40

So it's actually a two-fold attack where they're stealing the information and then altering it to give themselves a competitive advantage. 11:10:43 11:10:46 11:10:47

THE COURT: All right. So you can -- I assume this is encrypted traffic. 11:10:51 11:10:58

THE WITNESS: Well, that's the problem, is a lot of these pharmaceutical companies are utilizing the old technology, where they actually have to decrypt the traffic. And the attacker in this case was able to get the keys to the encryption, so they were able to decrypt all the information. 11:10:59 11:11:05 11:11:08 11:11:13 11:11:20

So this story highlights the problem with the old method; that your keys are laying around and attackers can steal the keys and decrypt your data. 11:11:23 11:11:25 11:11:29

THE COURT: Not only decrypt it but substitute false data for what was in there. Is that what you're saying? 11:11:32 11:11:40

THE WITNESS: Exactly. The key is just like the key to your house. If somebody can get into your house, they cannot only steal things, they can move your furniture around and change things. 11:11:43 11:11:45 11:11:49 11:11:53

So, yeah, the keys are critical, and that's why this '856 invention is so important; because it protects and secures the keys without decrypting the information. 11:11:54 11:11:57 11:12:01

THE COURT: Well, in this case it wouldn't do them any good unless they could decrypt, right? 11:12:10 11:12:15

THE WITNESS: Exactly. So if they -- 11:12:21

THE COURT: You said by using the old system, they enabled themselves to be attacked through decryption. 11:12:25 11:12:29

THE WITNESS: Correct, because they left the keys laying around, and the foreign adversary was able to get those keys and decrypt the information. 11:12:38 11:12:40 11:12:45

THE COURT: So if they would have used -- what you're saying is if they would have used this new system, they wouldn't have been able to decrypt it? Or it would have -- well, let's put it this way: 11:12:48 11:12:51 11:13:01 11:13:03

It would have gotten to the recipient in an unaltered form, at least? 11:13:05 11:13:08

THE WITNESS: Correct. In these cases, because of defense in depth, I always want to be careful, but at least the current way the attack happened, where they stole the key off the server, if the invention in the '856 patent was used, 11:13:09 11:13:16 11:13:20 11:13:25

the current attack -- that would not have been possible. 11:13:29

THE COURT: Okay. 11:13:36

BY MR. ANDRE: 11:13:36

Q. Doctor, I want to show you what's been marked as PTX-66. 11:13:37

MR. ANDRE: This is not admitted yet, Your Honor. 11:13:40

BY MR. ANDRE: 11:13:40

Q. Could you describe what this document is? 11:13:47

A. This is another presentation from one of Cisco's 11:13:48

principal engineers on Cognitive, and what it's really 11:13:56

referring to here is Cognitive Threat Analytics, and it's 11:14:01

giving an inside view of how it works. And, once again, the 11:14:04

date of this document is August 2018. 11:14:08

MR. ANDRE: Your Honor, I'd like to move PTX-66 into 11:14:13

evidence. 11:14:16

THE COURT: PTX-66 will be admitted. 11:14:19

(Plaintiff's Exhibit PTX-66 was received in 11:14:24

evidence.) 11:14:25

BY MR. ANDRE: 11:14:25

Q. Dr. Cole, I'd like to turn to Page 20 of this document. 11:14:26

Now, the figure above -- we've seen something 11:14:31

similar to that before. We won't -- is there anything new 11:14:34

you want to discuss about this? We can go there, or we can 11:14:38

just incorporate your last -- previous testimony. 11:14:43

A. Just real briefly, since it's up on the screen, this is 11:14:49

showing that we can inspect the encrypted traffic. 11:14:52

So if we start on the left-hand side, it's making the most of the unencrypted fields. So this is almost right out of the patent claim language, where it's using unencrypted fields to be able to determine if there's threats within the encrypted traffic. 11:14:56 11:14:59 11:15:03 11:15:07 11:15:11

And, once again, the big focus of Cisco with these documents, as you heard from Steven Rogers, the CEO of Centripetal, is it's all about the "who," the Who's Who of the internet dark side. It's not about the "what" anymore, it's about who's doing it, and that's exactly what the encrypted threat -- sorry -- Encrypted Traffic Analytics is doing. 11:15:13 11:15:17 11:15:23 11:15:26 11:15:29 11:15:31 11:15:35

Q. If we go down to the text on this page, it talks about the initial data packet, which you discussed earlier, and something called the "sequence of packet length and time and byte counts." 11:15:35 11:15:41 11:15:44 11:15:48

Could you just briefly describe what's being discussed there? 11:15:49 11:15:52

A. Yeah. So the first item, initial data packets, this is what we talked about, where, by looking at the Secure Socket Layer -- that's SSL -- or Transport Layer Security, or Hypertext Transfer Protocol Security -- so, just so we're clear, Secure Socket Layer, HTTPS, Hypertext Transfer Protocol Security, and Transport Layer Security, they're all referring to the same thing. There's just different versions 11:15:52 11:15:58 11:16:04 11:16:12 11:16:15 11:16:23 11:16:25

of it, but they're all referring to the same component, which is the initial setup of the encrypted traffic, and this is showing that we're using the unencrypted fields to do that analysis. 11:16:28 11:16:30 11:16:35 11:16:38

Then the second item -- and this is what Your Honor asked about in terms of packet lengths, times, and byte count, where now it can identify the content type, even though the data is encrypted, by measuring the size of the packets, the timing differences, and how they're delivered without actually decrypting any of the traffic. 11:16:39 11:16:45 11:16:49 11:16:53 11:16:57 11:17:02

Q. If we go back to the claim language, did the evidence you talked about today give you any opinion as to whether or not Cisco's accused systems infringe the determine, based on the portion of the unencrypted data corresponding to the network threat, have claim elements for both claims 24 and 25? 11:17:05 11:17:16 11:17:21 11:17:27 11:17:30

A. Not only with the documents that I've shown today but in all of the analysis that I've done for this case, it clearly shows that the infringing system from Cisco is able to determine, based on unencrypted data, threats in the encrypted portion without decrypting that information and clearly meets this claim element. So we can check this box. 11:17:34 11:17:37 11:17:41 11:17:45 11:17:49 11:17:53

Q. All right. Let's go to the last two claim elements on the next page. 11:17:56 11:18:02

Now, there's a -- on the introductory portion of this element, before you get to the sub elements, one appears 11:18:04 11:18:09

longer than the other. Could you describe to the Court what is the difference between the one on the left and the one on the right? And I think we have this highlighted. 11:18:14 11:18:16 11:18:18

A. The one on the right, claim 25, is computer-readable medium, and this just has a couple of clarifying words added to it. 11:18:21 11:18:26 11:18:32

So "by the packet-filtering system" is added with claim 25 because of the computer-readable medium, but if you read the claim in 24, it actually is implying that that's done by the packet-filtering system, so this is just a clarifying component. 11:18:33 11:18:39 11:18:42 11:18:48 11:18:52

And then, once again, claim 25 adds "indicating one or more of the plurality of network threat indicators," and, in my expert opinion, this is, once again, just clarifying that you have to pick one of these but not all of them. And this is also assigned with claim 24 because it has the word "or" at the bottom, showing that it's one of these, not all of these. 11:18:54 11:18:57 11:19:03 11:19:06 11:19:10 11:19:15 11:19:18

Q. Let's clarify that a little bit. 11:19:18

First of all, you're going to do filtering, correct? This is a filter element, correct? 11:19:24 11:19:27

A. Yes, this is a filtering element. And it looks like a really long element, but it's just naming a lot of the different components, and we have to go in and just show that one of these components is filtered on. 11:19:28 11:19:31 11:19:36 11:19:42

Q. There are five different possible ways of filtering in this claim element; is that correct? 11:19:44 11:19:49

A. That is correct. If you actually go through and count them up, starting with the "Uniform Resource Identifier" and finishing with "data indicating a command" there's actually five different things you can filter on. 11:19:50 11:19:53 11:19:57 11:20:04

Q. When we talk about filtering, is that just what the routers and switches do as packets come through; they just filter packets? 11:20:07 11:20:10 11:20:13

A. Yes. Essentially, it's looking for, analyzing, or filtering on a certain field or a certain information. So it could be as simple as if we're watching cars going down the street, we might filter on the color of the car, or we might filter on some other component associated with that automobile. 11:20:14 11:20:18 11:20:21 11:20:27 11:20:31 11:20:34

Q. Okay. For your testimony today, I would like to -- I don't want to do all five of these elements. We only have to prove one. Is it okay if we put in evidence to show the first two, anyway? 11:20:34 11:20:40 11:20:43 11:20:46

A. Yeah. So we'll show today -- just because of time and to keep this concise, we'll focus on the Uniform Resource Identifier, which includes a domain name, and then we'll also focus on data indicating the protocol version. In this case that's Transport Layer Security, TLS, or SSL, Secure Socket Layer protocol version. 11:20:48 11:20:53 11:20:58 11:21:02 11:21:07 11:21:13

Q. All right. Let's start with PTX-570. 11:21:16

MR. ANDRE: Your Honor, this has been admitted into evidence already. 11:21:25 11:21:27

BY MR. ANDRE: 11:21:27

Q. Dr. Cole, I'd like to turn your attention to Page 51 of the document. 11:21:31 11:21:34

MR. ANDRE: Beginning at Bates number 640, Your Honor. 11:21:34 11:21:39

BY MR. ANDRE: 11:21:40

Q. And focus on the table, the bottom table. 11:21:42

Could you describe to the Court what this table is discussing. 11:21:50 11:21:54

A. Sure. So, first, if we look in the upper right-hand corner, it has a red box around it. It has filter results. So this shows me that the system has the capability of filtering results, which is the exact claim language. 11:21:54 11:21:59 11:22:05 11:22:09

And if we go and look at the first column, encryption, TLS, which is Transport Layer Security, and SSL, which is Secure Socket Layer version, this is the protocol version. So this is, once again, right out of the claim language, and so this clearly shows that you can filter based on the protocol version. 11:22:12 11:22:17 11:22:23 11:22:27 11:22:30 11:22:34

THE COURT: "Filter based on the protocol version." That means that the rule could tell you to let the packet pass or not? 11:22:38 11:22:41 11:22:48

THE WITNESS: So filtering on the protocol version, that would let us get a little bit more specific. 11:22:48 11:22:54

So, for example, I can filter on Transport Layer Security version 1.2, so only show me traffic or only filter traffic on Transport Layer Security version 1.2. So we're using protocol version, so it will let you filter on the specific version of the protocol. 11:22:58 11:23:01 11:23:06 11:23:11 11:23:14

BY MR. ANDRE: 11:23:22

Q. All right. If we turn to -- 11:23:23

THE COURT: Well, wait a minute. 11:23:25

So the protocol, that's the policy? It's the same as a protocol? I mean, a protocol includes a series of rules, and what you're saying is you can filter it based on any one of those rules, as opposed to using all of them or more than one of them. 11:23:31 11:23:40 11:23:45 11:23:48 11:23:52

THE WITNESS: Right. So for this claim element, we're showing filtering on the protocol version, and then the protocol version is one of the components that could actually be in a rule that we'll get to a little later on in the claim elements. 11:23:57 11:23:59 11:24:04 11:24:09 11:24:15

THE COURT: Okay. 11:24:18

BY MR. ANDRE: 11:24:19

Q. If we go to PTX-578 -- 11:24:21

MR. ANDRE: This has been admitted earlier today, Your Honor. 11:24:28 11:24:31

BY MR. ANDRE: 11:24:31
Q. -- and go to Page 17, ending in Bates number 067, could you describe how this informed your opinion as to filtering based on the different protocol versions? 11:24:32 11:24:38 11:24:41
A. Yes. So the claim element says that you need to filter based on one of five elements, one of those being the protocol version, and here this slide is clearly showing filtering the flows by protocol version. 11:24:44 11:24:52 11:24:55 11:24:58
Transport Layer Security, TLS, and Secure Socket Layer are protocols, and you can see in the lower right-hand corner, under "Encrypted Version," that you're actually able to filter on those protocol versions. So, once again, this slide is almost directly aligned with the claim language, showing that the Cisco infringing systems have the capability to filter based on protocol version. 11:25:04 11:25:08 11:25:12 11:25:17 11:25:21 11:25:24 11:25:28
THE COURT: What does "protocol version" mean? How does that fit in with the concept of policies and rules? I don't understand. Is protocol version a subsection of a rule? What is it? 11:25:31 11:25:40 11:25:46 11:25:52
THE WITNESS: So you have protocols which specify how communication occurs, and over time you enhance those. So you start off with version 1, and then you might go in and add more components for version 2, version 3. 11:25:53 11:25:59 11:26:06 11:26:10
An example would be your home computer or your work computer. You might have a Windows operating system that has 11:26:13 11:26:19

different versions. I don't know if you remember Windows NT, and then you had Windows XP and Windows 7 and Windows 10. 11:26:23 11:26:27

THE COURT: And as soon as we learned one of them, they changed it. 11:26:32 11:26:34

THE WITNESS: Exactly. You're right. That's how Microsoft has to make money. 11:26:36 11:26:38

But those are different versions of the software that they keep enhancing and changing. So protocols are the same way, where you have different versions of the protocol. So you might have version 1, version 1.2, version 2. 11:26:40 11:26:44 11:26:48 11:26:52

And then, to specifically answer your question, the protocol versions that you're filtering on then would become a specific component of the rules. 11:26:56 11:27:00 11:27:03

THE COURT: A component of the rules. So it's a subsection of the rules. 11:27:08 11:27:13

THE WITNESS: Right. So one of the things in the rules that you might do is filter on a specific version of the protocol. 11:27:15 11:27:17 11:27:20

THE COURT: Well, what are protocols filtering, threat intelligence? Is that what they're filtering based on? 11:27:29 11:27:35 11:27:39

THE WITNESS: So the filtering could be done on threat intelligence, but it could also be something as simple as if there's an older version of the protocol, say version 1.0, that might have more vulnerabilities in it, we might 11:27:42 11:27:47 11:27:50 11:27:57

want to set up a rule to be able to filter on that older version of that protocol. 11:28:02 11:28:06

BY MR. ANDRE: 11:28:12

Q. What is a protocol, Dr. Cole? 11:28:12

A. A protocol is rules of engagement. It essentially specifies how two computers can work together in order to communicate back and forth. 11:28:14 11:28:21 11:28:27

A simple example is a language. Right now we're using the protocol of the English language. You're asking questions in English, and, hopefully, most of the time I'm responding in English and not technical terms. But we're speaking a rule of engagement to communicate, and that's all a protocol is, is just rules of engagement for two computers to be able to set up communication, or in this case, with Transport Layer Security or Secure Socket Layer, it's rules that they would use to set up an encrypted channel between the two systems. 11:28:28 11:28:32 11:28:35 11:28:39 11:28:43 11:28:46 11:28:51 11:28:54 11:28:58 11:29:02

Q. And might it be that an older version of the protocol would be more vulnerable to attack? You might want to filter on different versions for that reason? 11:29:04 11:29:07 11:29:11

A. Exactly. One of the many reasons why you come out with new versions of protocols, why you would have version 2 or version 3, is to not only enhance performance and functionality, but it's also to fix vulnerabilities and exposures that are present in earlier versions of the 11:29:12 11:29:16 11:29:20 11:29:23 11:29:27

protocol.

THE COURT: Or it may be something as simple as changing the language. 11:29:30 11:29:31 11:29:35

THE WITNESS: Exactly. 11:29:36

THE COURT: Okay. 11:29:40

MR. ANDRE: Your Honor, do you want to take our morning break now, or should I continue? 11:29:41 11:29:42

THE COURT: Well, yes, this would be a good time to take the break. Let's adjourn until 11:45. 11:29:46 11:29:49

(There was a recess from 11:30 a.m. to 11:46 a.m.) 11:38:30

THE COURT: All right, Mr. Andre. You may continue. 11:46:24

MR. ANDRE: Thank you, Your Honor. 11:46:28

BY MR. ANDRE: 11:46:29

Q. Dr. Cole, we were just talking about the filtering, and you gave a few examples of filtering based on protocol versions. 11:46:30 11:46:33 11:46:36

You previously provided testimony of filtering based on the URI or Uniform Resource Identifier. What is included in a Uniform Resource Identifier? 11:46:37 11:46:42 11:46:48

A. One of the things that's included in a Uniform Resource Identifier is a domain name. So a domain name is one of the key Universal Resource Identifiers that we utilize. 11:46:50 11:46:54 11:47:00

Q. And you've provided evidence previously about how the systems filter through on domain names? 11:47:04 11:47:06

A. Yes. We showed several pieces of evidence showing domain 11:47:11

names, even some testing that I perform that utilized domain names. 11:47:14 11:47:19

Q. Let me show you one exhibit that's not in evidence yet referring to that, PTX-996. 11:47:19 11:47:22

Dr. Cole, what is this document? 11:47:27

A. This is a Cisco Stealthwatch Configuration Guide, so this shows how to configure and utilize their product. 11:47:32 11:47:36

MR. ANDRE: Your Honor, I'd like to move PTX-996 into evidence. 11:47:39 11:47:42

THE COURT: Now, I didn't hear. You said this shows how to filter something, Doctor, 996? 11:47:53 11:48:00

THE WITNESS: Sorry. 996 is a configuration guide, so it shows how to configure the Cisco Stealthwatch. And one of the things that it shows in this guide that we'll go to is that it can filter on domain names. 11:48:04 11:48:10 11:48:14 11:48:18

BY MR. ANDRE: 11:48:30

Q. This document, on the second page, is copyrighted 2019. Does that sound correct, Dr. Cole? 11:48:30 11:48:37

A. Yes, that looks to appear to be the correct date. 11:48:39

THE COURT: What date? 11:48:41

MR. ANDRE: Copyright 2019, Your Honor. 11:48:42

THE COURT: Okay. 11:48:53

BY MR. ANDRE: 11:48:53

Q. If we go to -- 11:48:56

MR. ANDRE: Your Honor, I'd like to admit PTX-996 11:48:57

into evidence.

THE COURT: That will be admitted.

(Plaintiff's Exhibit PTX-996 was received in evidence.)

BY MR. ANDRE:

Q. If we go to Page 5 of this document, ending in Bates number 005, and just pull up the first half of that, where it talks about ETA flow records.

Dr. Cole, could you explain how this informs your opinion as to filtering based on the URI, or Uniform Resource Identifier.

A. So this is showing the Encrypted Traffic Analytics flow records, and this can include the initial data packet, the Transport Layer Security session ID, the cipher suites, the sequence of packet lengths and times, and the Transport Layer Security version.

And if you go in and look under the asterisk under initial data packet, this says it contains mostly protocol-related data and headers, such as server name indication. So that is -- server name or domain name is a component of the Uniform Resource Identifier.

Q. If we go back to the claim language, based on all the evidence you presented here today talking about this element and previous elements, your testing, your review of the source code, did you form an opinion of whether or not the

accused Cisco systems infringe the filter element in claims 24 and 25? 11:50:33 11:50:38

A. Yes. Based on the previous evidence and the evidence we've just shown before break, the system can clearly filter based on a Uniform Resource Identifier, specifically the domain name, and also on protocol versions. So these claimed elements for both 24 and 25 are met, and we can check the box. 11:50:38 11:50:44 11:50:47 11:50:51 11:50:56 11:51:00

Q. All right. Let's turn to the last claim element, the routing. This is routing by the packet-filtering system, filter packets to a proxy system, based on determination that the filter packets comprising data that correspond to one or more network threat indicators. 11:51:00 11:51:09 11:51:13 11:51:16 11:51:19

Could you explain what you were looking for when you were doing your analysis of this element. 11:51:22 11:51:25

A. Yes. So we were looking for the ability to route packets, and the way that's done -- and we briefly mentioned it in my introduction, but we'll clearly show more evidence, after I describe this, that that's done by Stealthwatch communicating to the Identity Service Engine, which has sometimes been referred to as I-S-E, or ISE, and then that can send routes to the routers and switches, with one of the cases being a quarantine, and that can then filter packets to a proxy system, which in this case would be the null interface on the router or the switch. 11:51:27 11:51:33 11:51:39 11:51:42 11:51:45 11:51:48 11:51:54 11:51:59 11:52:05 11:52:09

And, once again, just to confirm, I utilized the Court's claim construction of proxy system in this case. 11:52:11 11:52:14

Q. Let's start off by looking at some of the testimony of Mr. Amin, Cisco's principal engineer. 11:52:18 11:52:25

MR. ANDRE: And, Your Honor, this is PTX-1927. This is not in evidence. I'd like to move PTX-1927 into evidence. 11:52:28 11:52:32

THE COURT: All right. PTX-1927, which is Amin again, will be admitted. 11:52:41 11:52:52

(Plaintiff's Exhibit PTX-1927 was received in evidence.) 11:53:13 11:53:13

BY MR. ANDRE: 11:53:13

Q. Dr. Cole, how did Mr. Amin's testimony inform your opinion as to this claim element of routing? 11:53:14 11:53:18

A. So he's asked whether Stealthwatch can send messages to the Cisco Catalyst switches, and he says, "I believe that's true." And then when he's asked, "What would the Cisco Catalyst switches do in response to the message from Stealthwatch," he says, "It may route packets in a particular way." 11:53:21 11:53:27 11:53:31 11:53:35 11:53:37 11:53:41

So, just pausing for a second, this confirms the first part of the claim element, where it has to be able to route packets. So Mr. Amin clearly shows that it has the ability to route packets in a particular way, and then, when asked in what way would the Catalyst switches route packets based on the methods of Stealthwatch, he says an example 11:53:42 11:53:46 11:53:49 11:53:54 11:53:58 11:54:02

would be to drop packets; for example, to not forward them. 11:54:05

And while he doesn't specifically say routing to a proxy system, if you look at the Court's claim construction, a proxy system misaligns with a system that intervenes between two hosts, so his answer aligns with the Court's construction of proxy system. 11:54:11 11:54:15 11:54:19 11:54:24 11:54:28

So his two answers confirm that the system, infringing system, aligns with the patent claim element. 11:54:30 11:54:33

Q. If we go to PTX-584... 11:54:36

Dr. Cole, when this document comes up, could you describe what this document is? 11:54:42 11:54:50

THE COURT: What was that number? 11:54:52

MR. ANDRE: PTX-584. 11:54:54

THE COURT: Is that already in evidence? 11:55:00

MR. ANDRE: It's not. I want to lay some foundation and move it in through Dr. Cole. 11:55:02 11:55:04

BY MR. ANDRE: 11:55:08

Q. Dr. Cole, what is this document? 11:55:09

A. This is a Cisco public white paper in which they are discussing Cisco Encrypted Traffic Analytics. 11:55:10 11:55:15

Q. And at the bottom left-hand corner is a copyright date of 2019 in fine print. Do you see that? 11:55:18 11:55:22

A. Yes, it looks to be 2019. 11:55:25

MR. ANDRE: Your Honor, I'd like to move PTX-584 into evidence. 11:55:29 11:55:32

THE COURT: That will be admitted. 11:55:33

(Plaintiff's Exhibit PTX-584 was received in evidence.) 11:55:33 11:55:34

BY MR. ANDRE: 11:55:34

Q. If we go to Page 6 of this document, bearing Bates numbers ending in 403, the bottom paragraph talks about, "Upon discovery, a malicious encrypted flow can be blocked or quarantined." 11:55:35 11:55:39 11:55:47 11:55:50

Do you see that? 11:55:51

A. Yes, I do. 11:55:52

Q. Could you describe to the Court how this document informs your opinion as to the last claim element of the '856 patent, claims 24 and 25? 11:55:53 11:55:57 11:56:01

A. Once again, this aligns very closely with the claim language, saying once it's identified malicious encrypted flow -- which, as a reminder, was done without decrypting the traffic -- it can then be blocked or quarantined by Stealthwatch. And it says this is policy-driven remediation actions, using policy grid, using Cisco's Identity Service Engine, ISE, with Cisco TrustSec. 11:56:03 11:56:07 11:56:11 11:56:15 11:56:20 11:56:26 11:56:32

So this is showing the communication that from Stealthwatch it utilizes Identity Service Engine to then route packets to a proxy, which is just another way of saying blocking or quarantining those packets by Stealthwatch. 11:56:37 11:56:39 11:56:43 11:56:50

Q. I'd like to show you another piece of testimony from 11:56:58

Mr. Agrawal, Cisco's product line manager, and this is PTX-1928. 11:57:01 11:57:07

MR. ANDRE: Your Honor, I'd like to admit PTX-1928. 11:57:11

THE COURT: Just a moment. Let me find it. 11:57:15

All right. PTX-1928 will be admitted. 11:57:42

(Plaintiff's Exhibit PTX-1928 was received in evidence.) 11:58:06 11:58:07

BY MR. ANDRE: 11:58:07

Q. And, Dr. Cole, could you tell the Court how Mr. Agrawal's testimony informed your opinion as to this last claim element, and particularly the first part of the answers he provided. 11:58:08 11:58:12 11:58:15 11:58:20

A. Yes. This supports all the evidence we've seen so far, where when he's asked, "Is there an interface within Stealthwatch where a user can click to automatically quarantine based on detection of threats with Encrypted Traffic Analytics," and he says, "That is a -- we call that one-button quarantine, and it's a button in Stealthwatch." 11:58:21 11:58:24 11:58:27 11:58:30 11:58:37 11:58:41

So this confirms that there's that capability to route, and then, if you look at the answer, he says, "Stealthwatch is not doing the quarantining directly. It's done via communication with a component such as ISE, Identity Service Engine." 11:58:44 11:58:47 11:58:50 11:58:52 11:58:58

So this confirms how the infringing scenario with Stealthwatch identifies the threats and encrypted traffic, 11:58:59 11:59:02

communicates with Identity Service Engine, that then sends a message to the routers or switches to route the packet to a proxy, which in this case would be a null interface. 11:59:06 11:59:12 11:59:15

THE COURT: Well, what is this "click" talking about here? What does that mean? 11:59:19 11:59:24

THE WITNESS: I'm sorry, Your Honor. I didn't hear the question. 11:59:26 11:59:31

THE COURT: What does "click" mean? Does this mean something has to be done manually? 11:59:31 11:59:35

THE WITNESS: The one option here is that there is a one-button quarantine, so the user could go in and click that one button, and then that would automatically do the quarantining, but the software for doing all of that quarantining is built into the system. 11:59:40 11:59:42 11:59:47 11:59:50 11:59:54

THE COURT: So nobody -- you don't have to use the manual option? If you don't use the manual option, it will do it anyway? 11:59:59 12:00:03 12:00:09

THE WITNESS: Correct. He's just giving one option here, but there's also an automatic way to do that, also. 12:00:11 12:00:12

THE COURT: All right. Well, can I see the rest of the language on this? 12:00:15 12:00:17

(There was a pause in the proceedings.) 12:01:05

THE COURT: Okay. 12:01:05

BY MR. ANDRE: 12:01:06

Q. Dr. Cole, you talk about the "null interface." I'd like 12:01:06

to show you PTX-526. 12:01:09

MR. ANDRE: And this is not in evidence yet, Your Honor. 12:01:12

BY MR. ANDRE: 12:01:14

Q. Dr. Cole, what is this document? 12:01:14

A. This is a Cisco community document, so this is a public document that they share. You can see the URL at the bottom of the screen, and this talks about the null interface that's built into routers and switches. 12:01:15

THE COURT: Just a minute. What is this number? 12:01:30

MR. ANDRE: PTX-256. 12:01:32

THE COURT: Okay. 12:01:35

MR. ANDRE: Your Honor, I'd like to move PTX-256 into evidence. 12:01:35

THE COURT: What was the question and the answer to Dr. Cole? I didn't get that. 12:01:45

MR. ANDRE: The question was what is this document referring to? 12:01:47

THE COURT: Can you give us your answer? 12:02:01

THE WITNESS: Yes. This is a Cisco community document. So these are public documents that Cisco provides to give details about their product. 12:02:05

In this case, they're talking about a feature that's in their switches and routers called the "null interface," which, as we'll see as we go through my explanation, serves 12:02:07

12:02:09

12:02:12

12:02:13

12:02:17

12:02:22

12:02:24

12:02:27

12:02:31

the role as a proxy. 12:02:35

THE COURT: So if it's dropped, it goes to the proxy? 12:02:47 12:02:49

THE WITNESS: Yes. If it's dropped, it would be routed to the proxy, which would be the null interface, and that, in essence, would drop the packet. 12:02:50 12:02:55 12:03:01

BY MR. ANDRE: 12:03:03

Q. And is that similar to quarantining the packet, as well? 12:03:08

A. Yes, that is. 12:03:10

THE COURT: All right. Go ahead. 12:03:14

MR. ANDRE: Your Honor, can I get 256 admitted into evidence? 12:03:17 12:03:21

THE COURT: That will be admitted. 12:03:22

(Plaintiff's Exhibit PTX-256 was received in evidence.) 12:03:22 12:03:23

BY MR. ANDRE: 12:03:23

Q. Turn to the second page. There's a description under number 1. 12:03:24 12:03:28

Could you describe what this document is discussing here? 12:03:29 12:03:31

A. Yes. So this is talking about a description of the null interface, where it's saying, "Only interface configuration command that you specify for the null interface..." and it then -- it's basically saying it's going to drop the packet, and then what action do you want to perform when it drops the 12:03:32 12:03:38 12:03:42 12:03:45 12:03:49

packet? 12:03:53

So you can send a message back to the host saying 12:03:53
that the system is unreachable, or you can direct packets 12:03:57
that will prevent the router from sending an internet control 12:04:02
message protocol. 12:04:07

So I know there's a lot of technical language in 12:04:08
here, but, essentially, what this is saying is the null 12:04:11
interface is a way that you route packets in order for it to 12:04:15
intervene in order to drop those packets. So you see that at 12:04:19
the end, packets destined for a particular network to be 12:04:24
dropped, and then you can go in and specify what message you 12:04:27
give back to the originating system. 12:04:32

But this shows -- and it's very well-known -- that 12:04:34
the null interface is a way to drop packets, intervening 12:04:37
between two systems playing the role of a proxy. 12:04:43

Q. And is the null interface something that is well-known in 12:04:46
your industry; how to -- a way to route packages away from 12:04:49
the original intended host? 12:04:53

A. Yes, it is. 12:04:55

Q. I'd like to show you one more piece of deposition 12:04:56
testimony from a Cisco software engineer, Mr. Llewallyn, and 12:05:02
this is PTX-1929. 12:05:11

MR. ANDRE: Your Honor, I'd like to admit PTX-1929 12:05:13
into evidence. 12:05:16

THE COURT: PTX-1929. 12:05:34

(Plaintiff's Exhibit PTX-1929 was received in evidence.) 12:05:34 12:05:50

MR. ANDRE: Thank you, Your Honor 12:05:50

BY MR. ANDRE: 12:05:50

Q. Dr. Cole, what did this testimony -- how did it inform your opinion as to the routing element? 12:05:51 12:05:56

A. So he's asked about Identity Service Engine, and, just as a refresher, Stealthwatch communicates with Identity Service Engine to then send messages to the router or switch to route to the proxy, and when he's asked about ISE, he says it has the ability to quarantine users. 12:05:57 12:06:05 12:06:10 12:06:14 12:06:19

So on the fourth line: "So the one thing that Stealthwatch can do based on the user, the administrator choosing to do so, is to quarantine a host." 12:06:22 12:06:25 12:06:29

So he's talking about the ability to quarantine or route packets to a proxy, such as the null interface. 12:06:33 12:06:36

Q. Thank you, Doctor. 12:06:39

THE COURT: You said "quarantine users." That means users are potential recipients of the packet, right? 12:06:57 12:07:04

THE WITNESS: Correct. So the user is the one that's actually performing some action on a computer that generates the packets that are encrypted over the network. So you can have different levels of abstraction, but one thing he's saying is you can decide that the encrypted traffic is bad based on the user activity and then go in 12:07:09 12:07:15 12:07:19 12:07:24 12:07:29 12:07:32

and -- 12:07:36

THE COURT: Well, somebody said "host." Who's the 12:07:37

host? 12:07:41

THE WITNESS: The host is the computer, and then the 12:07:41

user is the person utilizing that computer. 12:07:47

THE COURT: Is this person the person who sends the 12:07:56

packet or receives it? 12:08:03

THE WITNESS: So it could be either one, but 12:08:06

typically, in this case, it would be a user is at a computer 12:08:08

system, and let's say their account, their user account, gets 12:08:14

compromised and it starts doing malicious activity out on the 12:08:20

internet. They can go in and identify, based on looking at 12:08:24

the encrypted traffic, without decrypting it, that that user 12:08:28

is doing something malicious, and they can identify the 12:08:32

address of the host and then quarantine that host address to 12:08:36

a proxy so that system can no longer do damage. 12:08:41

THE COURT: Well, that sounds like you're talking 12:08:47

about the recipient being a bad guy and you can keep him from 12:08:49

receiving it. 12:08:57

Are you saying that you can also use this technology 12:08:59

to quarantine the source? 12:09:03

THE WITNESS: Yes, you can have two scenarios. So 12:09:07

one scenario is what you just mentioned, where the recipient 12:09:12

breaks into a host and extracts information out of it, but 12:09:20

you could also have a scenario that we call in cyber security 12:09:23

a "bad actor," and that can be somebody inside the company that is working for a competitor or wants to cause harm, and they can go in, that user, to try to deliberately send information out of the organization. They could also identify that bad actor and then quarantine that host to a proxy. 12:09:26 12:09:31 12:09:37 12:09:42 12:09:44 12:09:51

THE COURT: So you could quarantine anyone in the chain of transporting the packet; the source, an intermediary or the intended recipient. Any of those could be quarantined. Is that what you're saying? 12:09:54 12:10:03 12:10:14 12:10:16

THE WITNESS: Yes. For this specific patent and the testimony here, we're really referring to more of the originating host, but you are correct; it could be either side that's doing damage and trying to cover it by utilizing encryption. 12:10:19 12:10:24 12:10:28 12:10:32 12:10:39

MR. ANDRE: May I proceed, Your Honor? 12:10:48

THE COURT: Well, I'm trying to figure out -- you said you could quarantine a bad actor within the company who's the recipient of the packet. 12:10:49 12:10:52 12:10:59

THE WITNESS: So if we look at a simple example, let's say somebody that works at the courthouse, they're a bad actor, and they're trying to connect to a malicious host out on the internet to exfiltrate out court documents, and they're utilizing encryption to try to cover their tracks. 12:11:09 12:11:12 12:11:19 12:11:24 12:11:31

In this case, it would be able to detect that that 12:11:37

bad actor, who is an employee of the court, is connecting to that site on the internet and then, once it determines that, then route them to a proxy that would quarantine or block them from doing further damage. 12:11:40 12:11:45 12:11:51 12:11:57

THE COURT: And it could also do the same thing to the source. 12:12:02 12:12:05

THE WITNESS: That is correct. 12:12:09

THE COURT: Or the intended recipient. 12:12:11

THE WITNESS: That is correct. 12:12:18

THE COURT: Okay. 12:12:20

BY MR. ANDRE: 12:12:23

Q. Dr. Cole, I want to show you one last piece of source code. 12:12:23 12:12:27

MR. ANDRE: Your Honor, I'd like to seal the courtroom for just a few minutes. 12:12:27 12:12:30

THE COURT: All right. 12:12:31

MR. ANDRE: And, Mr. Rogers, please step out for about five minutes. 12:12:38 12:12:40

We have confirmation Mr. Rogers stepped out. 12:12:45

(Confidential testimony from Page 970, Line 20, through Page 972, Line 15, was redacted.) 10:53:50 10:53:50

* * * * * * * 12:12:50

12:12:50

(Confidential testimony from Page 970, Line 20, through Page 972, Line 15, was redacted.)

* * * * * * *

BY MR. ANDRE: 12:15:34

Q. Dr. Cole, can we go back to the claim language? 12:15:35

A. Yes, we can. 12:15:37

Q. Based on the exhibits you showed here today, your testing, the source code you reviewed, did you form an opinion as to whether or not the Cisco accused systems infringed the last claim element of claims 24 and 25 of the '856 patent? 12:15:38 12:15:41 12:15:44 12:15:49 12:15:52

A. Yes, we saw with the evidence that it can actually route filtered packets to a proxy system, in this case the null 12:15:55 12:15:58

interface, based on encrypted traffic that contains network threat indicators. So we proved this element, and we can check that box. 12:16:02 12:16:05 12:16:08

Q. Dr. Cole, at this time you've checked all the claim elements of claims 24 and 25 of the '856 patent, as it relates to the accused systems that we have in this case. 12:16:09 12:16:16 12:16:20

Would you give your final conclusion as to your opinion as to whether or not the accused switches and routers, along with Stealthwatch and the Identity Service Engine infringe claims 24 and 25? 12:16:23 12:16:26 12:16:29 12:16:33

A. The identified technology, as you said, the accused routers and switches of Stealthwatch and Identity Service Engine, in my expert opinion, infringe claims 24 and 25 of the '856 patent. 12:16:35 12:16:38 12:16:43 12:16:47

Q. Thank you, Dr. Cole. 12:16:49

Now, let's turn to the second patent you're opining upon, the '176 patent. And what are we calling this patent? 12:16:51 12:16:54

A. This patent we call the correlation patent. 12:17:01

Q. Now, can you describe to me -- I know "correlation" has a specific meaning in computer science or cyber security. How would you describe "correlation" in a way that lay people would understand it? 12:17:08 12:17:11 12:17:15 12:17:20

A. Well, what you're doing is taking different pieces of information and putting it together to form a complete picture. 12:17:21 12:17:24 12:17:27

So an example would be if I come home from work today and I see somebody running through my neighborhood, that alone would not be indicative of suspicious activity. I might also see somebody carrying a box through my neighborhood. Once again, that by itself is okay. I might also see somebody wearing a hat, and I might see a police car just patrolling the neighborhood. Those individual activities by themselves are not suspicious or would raise concern or alarm. 12:17:27 12:17:31 12:17:35 12:17:41 12:17:44 12:17:47 12:17:52 12:17:58 12:18:03

However, if I go home tonight and I see somebody running through my neighborhood, wearing a ski mask, carrying a box, being chased by a police car, now I would be much more suspicious that something bad is going on. 12:18:03 12:18:07 12:18:10 12:18:15

So that illustrates the power of correlation, where you're taking individual events, putting them all together, to get a clearer picture of what is happening in an environment. And the same thing happens within a network. Attackers today are very clever, so individual activities by themselves might not be concerning, but when you start to correlate all of it together, just like I showed in the example, you can start to get a clearer picture of whether something is good or something is malicious. 12:18:18 12:18:21 12:18:25 12:18:27 12:18:32 12:18:36 12:18:39 12:18:43 12:18:46

Q. So let's turn to JTX-3, which is in evidence. This is the '176 patent. 12:18:48 12:18:54

If we could turn to -- this is claim 11. Could you 12:18:57

describe generally what claim 11 is covering? 12:19:05
A. What claim 11 is covering is you have a device, such as a router or a switch, and it's receiving packets that are coming in, and it's generating logs. The packets are then transmitted out of the router or switch, it's generating logs again, and then it correlates those logs together, and based on that correlation, it generates one or more rules that can then get provisioned back to a device on that first network. 12:19:08 12:19:15 12:19:20 12:19:25 12:19:30 12:19:34 12:19:41
Q. What was the summary of your opinions as to Cisco's accused systems in claims 11 and 21 of the '176 patent? 12:19:44 12:19:52
I'm sorry. Real quick, is claim 21 of the patent just the computer-readable medium version of the system? 12:19:56 12:20:00
A. Yes, except for the beginning preamble portion, which is just the computer-readable media that we've covered several times in this case, both by myself and by Dr. Mitzenmacher, the rest of the claims of 21 are identical to 11. 12:20:05 12:20:10 12:20:14 12:20:17
Q. Now let's go to the summary of your opinions as it relates to the '176 patent. 12:20:22 12:20:27
A. In this case, my opinion is that the accused Cisco switches and routers, along with Cisco's Stealthwatch, infringe claims 11 and 21 of the '176 patent. 12:20:28 12:20:31 12:20:35
Q. And using an animation we've been using here, could you describe, you know, in like a big picture, how this system works? 12:20:39 12:20:47 12:20:52
A. Sure. So, as we discussed, your routers and switches are 12:20:53

connecting networks together. So you have network 1 and network 2, and what's happening here is, as a packet in the animation is going from network 2, it's received by the routers and switches running Encrypted Traffic Analytics, it generates logs, and then as it's sent out, it generates a second set of logs. So there's logs coming in when it's received and when it's sent out. Those are then correlated together, and then, based on that correlation, a rule is created that's sent out to a device on network 1. 12:21:01 12:21:04 12:21:10 12:21:15 12:21:18 12:21:22 12:21:26 12:21:30 12:21:34

Q. All right. Let's turn to the claim language. 12:21:39

Now, the first element here, could you describe, once again, very briefly, what we're discussing here? 12:21:52 12:21:56

A. Yes. For 11, this is a system claim, so this is almost identical to the language in '856, at least one processor and memory-storing instructions, and when executed by at least one processor. And, once again, we're referring to the same switches and routers that I did in '856 and the same switches and routers that Dr. Mitzenmacher covered over his three days of testimony. 12:21:58 12:22:06 12:22:12 12:22:16 12:22:19 12:22:23 12:22:28

And then 21 is computer-readable medium compromising instructions that, when executed by a computing system, cause the computing system to perform action. And, once again, this is very similar to '856 and what Dr. Mitzenmacher covered, talking about the switches and the routers. 12:22:29 12:22:34 12:22:38 12:22:41 12:22:45

Q. So, relying on your testimony previously today regarding 12:22:51

the Catalyst switches, the ASR and ISR routers, and exhibits previously admitted today -- PTX-524, PTX-573, and PTX-1008 -- did you form an opinion as to whether or not the accused Cisco's system and routers have at least one processor, memory, and a CRM, or computer-readable medium? 12:22:53 12:22:58 12:23:06 12:23:10 12:23:17

A. Yes. Using the exact same evidence that we showed earlier just as a quick refresher, those documents show that these routers and switches have processors, they have memory, they have hard drives, and those hard drives and memory store instructions that get executed on the system. Based on all of that previous evidence that we showed earlier today, both of these elements are met, and we can check these boxes. 12:23:23 12:23:26 12:23:30 12:23:33 12:23:36 12:23:41 12:23:44

Q. Okay. So the next four claim elements describe, essentially, two elements that are identical in a first network and a second network. 12:23:48 12:23:58 12:24:03

Can you describe what we're looking at with both these elements? 12:24:05 12:24:06

A. Yes. So you have your router or switch, and you have network 1, and when you're sending packets to network 1, it's initially received, and when it's received here, it then generates logs. It would then generate logs. 12:24:07 12:24:13 12:24:16 12:24:21

Then, when this router or switch takes that same packet and sends it out or is transmitting it, it's transmitting it out of the device, and then it generates logs again. 12:24:26 12:24:28 12:24:31 12:24:35

So, essentially, it's the same router or switch that receives the packet and generates logs and takes the packet, transmits it, and generates a second series of logs. So the activity is performed by the same device and is very similar; it's just one is receiving and one is transmitting. 12:24:37 12:24:39 12:24:44 12:24:48 12:24:51

But the activity of receiving and transmitting and generating the logs is the same activity, so in order to be concise, we're going to cover all four of those together, because it's the same device, the same technology, and it operates in a similar manner. 12:24:54 12:24:57 12:25:02 12:25:05 12:25:07

THE COURT: Does the system log in packets that are -- what was the language we used? -- sent to a proxy or just lets it go through? 12:25:10 12:25:23 12:25:28

THE WITNESS: So in this case, Your Honor, with the '176 patent, there's actually not a proxy in the claim language. So we don't actually have a proxy in this case. We just have to show that the router or switch receives packets and logs and transmits packets and logs. 12:25:35 12:25:37 12:25:40 12:25:44 12:25:47

BY MR. ANDRE: 12:25:52

Q. And, Dr. Cole, if it was being routed to a proxy, would it also generally log that it was routed to a proxy? And it's not in this claim language, but would it also create a log? 12:25:53 12:25:57 12:26:00 12:26:03

A. Yeah. So the host on network 1, it could have anything on network 2. So network 2 could be a server, or network 2 12:26:03 12:26:09

could be a proxy. So if you're sending packets to the proxy, even though it's not required by this claim element, that would still generate logs on the system. 12:26:13 12:26:17 12:26:21

THE COURT: Well, that's what I was asking about, because under the prior patent, where you correlate a series of acts which together constitute a threat, if you send something to the -- I keep forgetting that language. We're not dropping it, we're sending it to a proxy. That's the language. 12:26:23 12:26:27 12:26:39 12:26:49 12:26:56 12:27:00

If you leave the ones that are sent to a proxy out, then what's left may not be sufficient to identify the threat. But you're saying that the packets that are sent to a proxy are logged in, so they would be among those logged in, the sum total of which might indicate a threat. 12:27:00 12:27:05 12:27:12 12:27:22 12:27:30

THE WITNESS: That is correct, and that's very observant. Because you're right. If we were taking the threats and sending them to a proxy and we weren't logging that, we would be missing out on a very critical piece of information. So whether the packets are going to a proxy or a regular system, they're still logged on the routers or switches. 12:27:35 12:27:38 12:27:41 12:27:44 12:27:49 12:27:52 12:27:57

THE COURT: Okay. 12:28:01

BY MR. ANDRE: 12:28:02

Q. Let me show you just a couple of graphics and explain how packets come into a system and how they go out, how that data 12:28:03 12:28:06

that includes the log is collected. 12:28:11

What are some of the terms we're going to be talking about? 12:28:15 12:28:17

A. Okay. So we have these terms, "packet ingress," which I always remember it, because I teach a lot and the terms can get confusing, that ingress is input. So the "I" is input, so it's going into the router or switch. So this is a packet that's going into the router or switch. And when it goes in, packets are generated, which includes log data, and then when the packet leaves, packets egress -- and I always remember "E" as "exit." So packet egress is exiting the device. 12:28:17 12:28:23 12:28:26 12:28:32 12:28:35 12:28:38 12:28:43 12:28:49

It would then also go in and generate packet data that includes logs, and that would be true when it's packet egress. Whether it's going to another server or whether it's actually going to the proxy, we would still get those outbound packet egress logs on the system. 12:28:55 12:28:58 12:29:01 12:29:03 12:29:09

Q. And is either side of this router or server here -- are those two different networks this is connecting? Is that network 1 and network 2 we're talking about? 12:29:12 12:29:16 12:29:19

A. Yes. So on the left-hand side, we can call that network 1, and then on the right-hand side, we can call that network 2, so it aligns with the language of the patent. 12:29:21 12:29:26 12:29:30

Q. And that log information that goes up between the ingress and egress, does that provide different information? 12:29:34 12:29:40

A. Yes, it does. I'm trying not to get too technical, but 12:29:44

when a packet comes into a router or switch, some of that information can be altered. So when it leaves the router or switch, it could actually have a different header. So by comparing that header of the information when it enters verse when it leaves is very valuable in being able to correlate and understand threats. 12:29:50 12:29:54 12:29:59 12:30:04 12:30:08 12:30:12

Q. And this type of traffic, does it go both directions? So if it goes from right to left, would that be ingress in that direction and egress in the other direction? 12:30:13 12:30:18 12:30:23

A. That is correct, because it's a bidirectional communication, so it's not just unidirectional. It goes in both directions, and in both cases, regardless of the direction, when it comes in, it generates data that includes logs, and when it leaves or is transmitted out, it also generates data that includes logs. 12:30:25 12:30:27 12:30:32 12:30:35 12:30:39 12:30:44

Q. Now, let me show you some of your own -- your own personal testing of the switches and routers. 12:30:46 12:30:50

MR. ANDRE: And this is PTX-408, which is in evidence, and this is at Page 25, Your Honor, and this is ending in Bates number 650. 12:30:52 12:30:56 12:31:02

THE COURT: 408 is already in, right? 12:31:07

MR. ANDRE: Yes. This is just another page of this document. It's Dr. Cole's testing documents, and this is Page 25, ending in Bates number 650. 12:31:09 12:31:11 12:31:14

THE COURT: 650. Okay, I've got it. 12:31:18

BY MR. ANDRE: 12:31:29

Q. Okay. If you look at down towards paragraph 2, where it says, "Specify the egress and ingress details of the following," do you see that? 12:31:29 12:31:32 12:31:36

A. Yes, I do. 12:31:37

Q. Could you describe what your own testing provided and how it relates to this claim element? 12:31:38 12:31:42

A. Yes. When I test the products, I want to make sure I fully understand the products and how they work and operate. So products often contain help files and resources -- and that's what this is from -- and this resource clearly shows and confirms what I previously testified; that on routers and switches when you set policies, which can include logging, you can specify both egress or ingress for the logging or the policy. 12:31:44 12:31:47 12:31:50 12:31:55 12:32:00 12:32:05 12:32:08 12:32:14

Q. If we turn to PTX-1060, 1-0-6-0, could you describe what this document is? 12:32:14 12:32:33

A. This is the Encrypted Traffic Analytics Deployment Guide that was released December 2017 by Cisco. 12:32:33 12:32:39

THE COURT: Wait a minute. Is this a new exhibit? 12:32:44

MR. ANDRE: It is, Your Honor. I'd like to move 1060 into evidence. 12:32:54 12:32:58

THE COURT: It seems to me I've seen this before, Encrypted Traffic Analytics Deployment Guide. 12:33:07 12:33:10

MR. ANDRE: I believe you saw a later version. 12:33:16

There's been a couple versions of this, and there may have been a Stealthwatch deployment guide, as well. 12:33:18 12:33:21

THE COURT: Okay. 12:33:26

(Plaintiff's Exhibit PTX-1060 was received in evidence.) 12:33:27 12:33:31

THE WITNESS: As Mr. Andre pointed out, it was the same cover that you saw previously but a different version. 12:33:31 12:33:34

THE COURT: Okay. 12:33:38

BY MR. ANDRE: 12:33:39

Q. And, Doctor, on Page 6 of this document ending in Bates numbers 008, there's a figure there, and it's talking about NetFlow. Do you see that? 12:33:40 12:33:48 12:33:56

A. Yes, I do. 12:33:57

Q. Could you describe how this influenced your opinion as to the four elements we're talking about, the identifying packets from the first network and the second network and how it generates logs? 12:34:03 12:34:07 12:34:13 12:34:16

A. Yeah. So the logs that we're talking about in this case that are being generated is actually NetFlow information. NetFlow is Cisco's proprietary logging system, and NetFlow can also work in both directions. You can see that in the NetFlow generator, the arrows are going both directions, and this is also based on my testing; that you can go in with NetFlow and specify it for ingress logging and egress logging. And this shows some of the key records that is 12:34:17 12:34:22 12:34:26 12:34:34 12:34:40 12:34:44 12:34:47 12:34:50

actually logged, so this further supports, with my testing, that you can go in and generate logs when packets are received by the router or switch and when they're sent out by the router or switch. 12:34:53 12:34:56 12:35:00 12:35:04

Q. And that's an example of some of the logging information there where it says "NetFlow Record Key Fields"? 12:35:04 12:35:08

A. Yes, this contains some of the information, and this is some of the data that is in the header, such as the IP address, the ports, the protocols. I know in multiple times in this case there was the grouping of five, the source and destination IP address, the source and destination port, and the protocol, and that grouping of five is also information that's listed within the logs that are generated by NetFlow. 12:35:12 12:35:14 12:35:19 12:35:25 12:35:30 12:35:33 12:35:36

THE COURT: Well, there was some testimony that was objected to as not being relevant that one of Centripetal's products could not pick up NetFlow. 12:35:40 12:35:48 12:35:54

Now, NetFlow is based on history, right? NetFlow measures something that's already gone through the system? 12:36:03 12:36:15

THE WITNESS: NetFlow is logging information. So as the packet enters the system, it will generate logs on that packet, and then as it forwards the packet, the logs are sent up to Stealthwatch. And then as that packet leaves the system, the egress, it also generates NetFlow logs that are sent up to Stealthwatch. 12:36:18 12:36:22 12:36:28 12:36:34 12:36:38 12:36:41

BY MR. ANDRE: 12:36:42

Q. And, Dr. Cole, are there different types of flow data that are logs that can be used by different systems? We're talking about NetFlow here for Cisco, but are there other types of logging systems, as well? 12:36:55 12:36:59 12:37:02 12:37:05

A. Yes, there's many different types of logs that are out there. NetFlow is one example, Syslog is another example, and there could be several others out there that would all fit the logging criteria of the patent language. 12:37:06 12:37:11 12:37:15 12:37:18

Q. Do you recall Dr. Moore testifying that Centripetal's product can also record logging information as they go through the system? 12:37:21 12:37:27 12:37:29

A. I do remember Dr. Moore saying that. 12:37:30

THE COURT: Well, there was something different about NetFlow and other logging systems, but I can't recall what the difference was. But at the time that evidence was presented -- and, of course, we've had a lot of other evidence since then -- it seemed that NetFlow was based entirely on history gathered after the packet was received by the recipient, but this diagram indicates that NetFlow requires information as the packet moves through the system, so it picks up information along the way before it reaches the recipient. Is that correct? It picks up information along the way? 12:37:36 12:37:43 12:37:51 12:37:58 12:38:01 12:38:05 12:38:19 12:38:24 12:38:32 12:38:39 12:38:44

THE WITNESS: That is correct. And I think where the confusion might be is NetFlow can be used for two 12:38:45 12:38:49

purposes.

So as the packets are going across the system, NetFlow is generated in near real time. So it's generating logs on those packets, but those logs are then stored to keep an historical profile of what happened. So now I can go back and look at what happened over the last 24 hours by looking at the NetFlow because that historical data was stored as it was generated during the packet transmission.

THE COURT: Okay. You may proceed.

MR. ANDRE: Thank you.

BY MR. ANDRE:

Q. And if we go to Page 21 of this exhibit, on Bates numbers 023, there's an entry on the bottom part of the page where it talks about Catalyst 9300 and 9400 series switches, ETA, and at the second paragraph can you talk about how that supports your opinion that the log is doing NetFlow entries per switch on ingress and egress?

A. Yes. So the second paragraph is talking about the Catalyst series of switches, and if we look at the second line, it talks about the capabilities, the number of entries per switch, and it shows that it logs both on ingress and egress.

So this further supports my opinion that the routers and switches not only receive and send the packets, but they can generate NetFlow logs on both the ingress/receiving and

the egress/transmitting of those packets. 12:40:34

Q. Go to the next document, PTX-572. 12:40:37

MR. ANDRE: And this is not in evidence yet, Your Honor. 12:40:45 12:40:49

THE COURT: PTX-1060 was already in evidence? 12:40:52

MR. ANDRE: I asked to move it in, Your Honor, and I think we admitted it, but, if not, I would like to move it in. 12:40:55 12:40:59 12:41:01

THE COURT: All right. PTX-1060 will be admitted. 12:41:03

Now, what is the new exhibit number? 12:41:07

MR. ANDRE: PTX-572. 12:41:10

THE COURT: Has this been admitted? 12:41:13

MR. ANDRE: It has not, Your Honor. 12:41:15

BY MR. ANDRE: 12:41:19

Q. And, Dr. Cole, could you look at maybe the second page of this document. 12:41:20 12:41:22

What is this document? 12:41:24

A. This is a Cisco design document where it's talking about Stealthwatch, "Network as a Sensor with Stealthwatch and Stealthwatch Learning Networks for Threat Visibility and Defense Deployment Guide," and this is dated February 2017. 12:41:24 12:41:31 12:41:51 12:41:54

MR. ANDRE: Your Honor, I'd like to move PTX-572 into evidence. 12:41:44 12:41:47

THE COURT: All right. PTX-572 will be admitted. 12:42:12

(Plaintiff's Exhibit PTX-572 was received in 12:42:15

evidence.) 12:42:17

THE COURT: You're on Page 990 at this point? Bates -- 12:42:17 12:42:25

MR. ANDRE: Bates 762. That's 9718, the cover page, but the page we're going to focus on is Bates number ending in 762. 12:42:26 12:42:33 12:42:38

If we could blow up the portion of the document -- 12:42:45

THE COURT: Just a minute. And you're on Bates number what? 12:42:49 12:43:18

MR. ANDRE: 762. 12:43:19

BY MR. ANDRE: 12:43:42

Q. Dr. Cole, there's a section in the middle of that document called "Flow Record." Would you describe what's being discussed in Exhibit 572, as it relates to flow records, and how it informs your opinion as to these claim elements. 12:43:42 12:43:45 12:43:53 12:43:58 12:44:01

A. It's talking about the flow records that's actually gathered via the NetFlow process, and the key component is the last paragraph, where it says, "When you configure a flow record, you are telling the device to show all of the flow data traffic that enters" -- which is ingress -- "or leaves" -- egress -- "the device." 12:44:01 12:44:04 12:44:08 12:44:13 12:44:16 12:44:19

So, once again, this further supports that the NetFlow process or logging can be done both receiving and sending packets, which aligns directly with the claim 12:44:22 12:44:27 12:44:31

language. 12:44:36
Q. Let me show you one more document regarding NetFlow or 12:44:36
flow records. This is PTX-569. 12:44:45
MR. ANDRE: And this is not in evidence at this 12:44:49
time, Your Honor. 12:44:51
BY MR. ANDRE: 12:44:52
Q. Dr. Cole, could you tell me what this document is? 12:44:53
A. This is a Cisco public document that they give out to 12:44:56
their customers on configuring and troubleshooting NetFlow 12:45:01
for Cisco's Stealthwatch. 12:45:04
Q. And if you look down at the bottom of the page, it's 12:45:06
copyright 2018. Does that sound right? 12:45:12
A. That is correct. 12:45:16
MR. ANDRE: Your Honor, I would like to move PTX-569 12:45:18
into evidence. 12:45:21
THE COURT: That will be admitted. 12:45:24
(Plaintiff's Exhibit PTX-569 was received in 12:45:24
evidence.) 12:45:24
BY MR. ANDRE: 12:45:24
Q. If we go to the Page 5 of this document ending in Bates 12:45:26
numbers 272, there's a description of defining a flow record 12:45:33
at the bottom of the page. 12:45:38
Could you briefly explain what's being discussed 12:45:42
here when it defines what a flow record is. 12:45:45
A. So this is going in and talking about the flow records, 12:45:47

which is the logging information, and that you can match on certain fields. And it goes in and gives some examples of what you can match on the protocol, the source address or the destination address. 12:45:54 12:45:59 12:46:03 12:46:08

So that's showing that when a packet enters, you have a source address; when it leaves, you have a destination. So this further supports that it can generate records for both ingress and egress packets. 12:46:09 12:46:12 12:46:15 12:46:19

Q. Thank you, Doctor. 12:46:29

MR. ANDRE: Your Honor, I'd like to seal the courtroom for just a couple of minutes. I want to show one piece of source code regarding this issue. 12:46:32 12:46:33 12:46:36

THE COURT: Okay. 12:46:39

MR. ANDRE: We'll confirm that Mr. Rogers stepped out. 12:46:42 12:46:46

It's confirmed.

(Confidential testimony from Page 990, Line 17, through Page 992, Line 9, was redacted.

* * * * * * *

(Confidential testimony from Page 990, Line 17, through Page 992, Line 9, was redacted.

* * * * * * *

BY MR. ANDRE:

Q. If we go back to the claim language, Dr. Cole, could you walk through each one of these four elements and describe the evidence you just presented to the Court and your testing and other evidence you've seen and give your opinion as to each one of these four elements in order.

A. Yes. So we've seen that your routers and switches can identify a plurality of packet --

THE COURT: I don't have the claim language on my screen.

MR. ANDRE: Is it there now, Your Honor?

THE COURT: Yeah.

BY MR. ANDRE:

Q. All right. So, Dr. Cole, just start over and start with the first identify and describe the evidence you went over for each one of these claim elements.

A. Sure. So you have your routers and switches, and you have your network 1, and when packets are received by that network device coming from network 1, we showed that the routers and switches can receive those packets, so it meets that first claim element. 12:50:10 12:50:12 12:50:18 12:50:22 12:50:26

We also saw for the ingress, or the packets coming inbound, it can also generate logs via NetFlow, so it meets the second element. 12:50:28 12:50:32 12:50:38

And then when the packets leave that router or switch going to network 2, which is egress, or exiting the router or switch, it's able to identify those packets that are transmitted going to that second network, so that third element is met. 12:50:40 12:50:42 12:50:46 12:50:49 12:50:54

And then when that happens, it can also generate NetFlow logs on the information that's being transmitted out, which meets the fourth element. 12:50:55 12:50:59 12:51:02

Q. All four boxes are checked on those four elements? 12:51:04

A. That is correct. 12:51:09

Q. Okay. Let's go to the next claim element on the next page of the slide. This is correlating. 12:51:10 12:51:13

Could you describe generally what this claim element requires. 12:51:17 12:51:19

A. Okay. What this claim element requires is that you're taking the logs from network 1 that were received, and the logs from that are transmitted to network 2, and you now 12:51:20 12:51:24 12:51:29

correlate those two logs together. 12:51:35
Q. Let's go to PTX-1065, 1-0-6-5. 12:51:39
MR. ANDRE: I do not believe this document is in 12:51:50
evidence. 12:51:52
BY MR. ANDRE: 12:51:52
Q. Dr. Cole, what is this document? 12:51:53
A. This is an internal Cisco presentation from November 12:51:54
2017, titled "Cisco Stealthwatch with Cognitive Threat 12:51:58
Analytics." 12:52:03
MR. ANDRE: Your Honor, I'd like to move PTX-1065 12:52:08
into evidence. 12:52:12
THE COURT: All right. This is PTX-1065. What kind 12:52:29
of document is this? 12:52:45
THE WITNESS: This is an internal Cisco 12:52:45
presentation, given by their product manager and technical 12:52:50
marketing engineer. 12:52:53
THE COURT: November '17. Okay. 12:53:07
(Plaintiff's Exhibit PTX-1065 was received in 12:53:12
evidence.) 12:53:13
BY MR. ANDRE: 12:53:13
Q. Dr. Cole, I'd like to turn your attention to Page 5 of 12:53:14
this document bearing Bates numbers 005. 12:53:18
Look at the figure and the first paragraph and 12:53:25
describe what is being shown in the figure and in the 12:53:27
paragraph itself and how it relates to the correlating. 12:53:30

A. So if we start at the bottom, you have a Stealthwatch flow collector that's collecting NetFlow data that's coming between the different networks. It's then taking that information and sending it to Stealthwatch, in which they're doing analytics on that, and then based on the correlation of that information, it's just sending an alert to a device on the first network, which would be the Stealthwatch Management Console. 12:53:36 12:53:41 12:53:46 12:53:52 12:53:58 12:54:04 12:54:08 12:54:12

And I know that last part is the final element that we haven't gotten to yet, but since we have the complete diagram, I just wanted to show the entire flow of information. 12:54:13 12:54:16 12:54:19 12:54:22

What I want to focus on here is what's happening in that blue cloud, and to understand what is happening in that blue cloud, we look at the text below it, and it basically says, starting halfway through on the second line, "...the cloud-based analytics engine that correlates threat behavior seen in the enterprise with those seen globally." 12:54:23 12:54:26 12:54:30 12:54:35 12:54:38 12:54:43

So that's clearly showing that Stealthwatch, integrated with Cognitive Threat Analytics, performs correlation of the logs and the NetFlow data. 12:54:47 12:54:50 12:54:54

Q. And if we turn to the next exhibit, PTX-591 -- 12:54:57

THE COURT: Do you want that one admitted? 12:55:10

MR. ANDRE: I do, Your Honor, Exhibit 1065 into evidence, please. 12:55:12 12:55:17

(Plaintiff's Exhibit PTX-1065 was received in evidence.) 12:55:44 12:55:46

MR. ANDRE: We're now on PTX-591, Your Honor. 12:55:46

BY MR. ANDRE: 12:56:00

Q. Dr. Cole, what is PTX-591? 12:56:01

A. These are release notes for Stealthwatch System Version 6.10.3. When a vendor like Cisco releases a new version of a product, they often give release notes which talk about the updates, the changes, and the enhancements made to that current version. 12:56:03 12:56:09 12:56:14 12:56:17 12:56:21

MR. ANDRE: Your Honor, I'd like to get PTX-591 admitted into evidence. 12:56:24 12:56:27

THE COURT: PTX-591 will be admitted. 12:56:36

(Plaintiff's Exhibit PTX-591 was received in evidence.) 12:56:36 12:56:40

BY MR. ANDRE: 12:56:40

Q. Dr. Cole, I'd like to turn your attention to Page 4, ending in Bates number 522. 12:56:40 12:56:45

On the release notes it states -- the first paragraph under Superforest, the CTA, would you describe what's being discussed in that paragraph. 12:56:51 12:56:54 12:57:00

A. Yes. So this is talking about some of the enhancements. 12:57:01

"Cognitive Threat Analytics can now leverage detection from the analysis of WebFlow telemetry to improve the efficacy of analyzing NetFlow telemetry from 12:57:05 12:57:08 12:57:13

Stealthwatch."

And then it talks about the way this is accomplished is through correlation of both telemetry types. So this shows that it can correlate the logs, the telemetry data, from multiple sources.

Q. It says "telemetry." What's that referring to?

A. The "telemetry" is just another word for the NetFlow log information. So the NetFlow telemetry, the NetFlow logs, these are all synonymous terms, so this is another way of referring to logs. So when you see "NetFlow telemetry," that's a specific type of Cisco logs that are being generated.

Q. Let me show you one more document relating to this claim element. It's PTX-1009.

MR. ANDRE: And, Your Honor, this has been admitted into evidence, but I want to go to a page that has not been admitted yet.

BY MR. ANDRE:

Q. And, Doctor, would you just remind the Court what this document is?

A. These are release notes for Cognitive Intelligence, which is formerly Cognitive Threat Analytics, or CTA.

Q. I'd like to draw your attention to Page 9, ending in Bates number 009.

MR. ANDRE: And, Your Honor, I'd like to admit

Page 9 into evidence, of this document. 12:58:46

THE COURT: That will be admitted. 12:58:52

(Plaintiff's Exhibit PTX-1009, Page 9, was received in evidence.) 12:58:53 12:58:54

BY MR. ANDRE: 12:58:54

Q. And, Doctor, do you see a date? It says April 2018, and go down to the first bullet point. 12:58:55 12:58:59

Could you describe what was being added into Cognitive Threat Analytics in April 2018. 12:59:02 12:59:05

A. Yes. So this is showing that by April 2018 Cognitive Threat Analytics can now leverage the analysis of the logs. So telemetry and NetFlow telemetry, those are Cisco specialized logs. 12:59:07 12:59:14 12:59:20 12:59:24

So just doing some translation, the analysis of the logs and the NetFlow logs, it can now go in and correlate those telemetry types together, and this shows that in April 2018 they started doing this correlation of those logs. 12:59:25 12:59:29 12:59:33 12:59:36

Q. Go back to the claim language. 12:59:40

THE COURT: That means they can get the threat analysis from different third parties? 01:00:06 01:00:11

THE WITNESS: Sorry, Your Honor. Yeah, it can get information from third parties, but what this is really focusing on is it can take logs from different sources on the network. 01:00:17 01:00:23 01:00:25 01:00:30

So from the different components of Stealthwatch -- 01:00:31

so packets coming in and packets going out and WebFlow data -- it can take those different logs, and it can now correlate those together to be able to get better insight into what's happening in order to be able to catch threats on the network. 01:00:33 01:00:37 01:00:40 01:00:44 01:00:48

BY MR. ANDRE: 01:00:53

Q. If we go back to the claim language, Dr. Cole, based on the evidence that you just went over regarding correlation and the testing you've done, the source code you've reviewed, did you form an opinion as to whether or not the accused Cisco systems infringe the correlating elements of claims 11 and 21 of the '176 patent? 01:00:54 01:00:59 01:01:02 01:01:05 01:01:08 01:01:12

A. Yes. The infringing products absolutely correlate the logs of the data that was received and sent and clearly meets this claim element, so we can definitely check this box. 01:01:14 01:01:18 01:01:23

MR. ANDRE: Your Honor, we're down to our last claim element of this patent. I know it's lunchtime. Do you want to take a break for lunch and pick up this last element after lunch? 01:01:28 01:01:31 01:01:34 01:01:39

THE COURT: How long is it going to take you? 01:01:39

MR. ANDRE: About five or ten minutes. We can finish it. That's fine. 01:01:42 01:01:45

THE COURT: All right. Well, let's try to finish it, if you can do it in five or ten minutes. 01:01:46 01:01:47

MR. ANDRE: We'll go through it very quickly. 01:01:51

BY MR. ANDRE: 01:01:53

Q. Dr. Cole, what is the last claim element about here? 01:01:54

A. So what the claim element is saying is based on that correlation that was performed, you need to generate one or more rules that can identify packets on -- sorry -- that can identify packets received from a host on the first network and then provision a device on the first network. 01:01:57 01:02:03 01:02:06 01:02:12 01:02:15

So, essentially, there's two main components here. We have to show that there's a generating of rules and a provisioning of a device. 01:02:19 01:02:21 01:02:24

Q. Let's start off by looking at some source code. 01:02:26

MR. ANDRE: Your Honor, I'd like to seal the courtroom for just a couple minutes. 01:02:30 01:02:33

THE COURT: All right. 01:02:34

(Confidential testimony from Page 1000, Line 15, through Page 1001, Line 10, was redacted.) 01:02:34 01:02:34

* * * * * * * 01:02:40

01:02:40

(Confidential testimony from Page 1000, Line 15, through Page 1001, Line 10, was redacted.)

* * * * * * *

MR. ANDRE: Oh, did we move in Page 7 of the source code, Your Honor? 01:03:43 01:03:47

THE COURT: Yes. 01:03:48

MR. ANDRE: Okay. Thank you. 01:03:50

BY MR. ANDRE: 01:03:51

Q. If we go to PTX-1089 -- 01:03:51

MR. ANDRE: And, Your Honor, this is a Cisco manual. 01:04:00

BY MR. ANDRE: 01:04:00

Q. Dr. Cole, did you rely on this manual in forming your opinion? 01:04:11 01:04:14

A. Yes, I did. I'm just seeing the table of contents, but this does look to be one of the manuals I relied on. 01:04:14 01:04:19

MR. ANDRE: Your Honor, I'd like to move in PTX-1089. 01:04:22 01:04:26

THE WITNESS: That will be admitted. 01:04:27

(Plaintiff's Exhibit PTX-1089 was received in evidence.) 01:04:29 01:04:30

BY MR. ANDRE: 01:04:30

Q. And I'd like to first turn your attention to the page bearing Bates number 1238. 01:04:31 01:04:34

And that figure that's in the middle of the page there, Step 0, there's suspicious behavior noticed for host, is that the source code you just showed with the suspicious behavior and the host? 01:04:43 01:04:49 01:04:53 01:04:57

A. Yes, that is. 01:04:58

Q. Okay. So what happens when they realize that there's some suspicious behavior noticed for the host? 01:04:59 01:05:02

A. It can go in and send a policy, which can also be thought of as rules, to take some action, in this case to quarantine a specific IP address. So then that message can be sent to either the Identity Service Engine, or that message could be sent to the Stealthwatch Management Console that's on network 1. 01:05:04 01:05:10 01:05:15 01:05:21 01:05:25 01:05:30

And the important thing here is it's focusing on an IP address, so the language of the claim says that it has to identify a specific host on network 1 and provision a device on network 1. So this is showing the identification of a rule for a specific IP address that's on network 1, and then it's able to send that quarantine policy to a device on network 1, which could be Identity Service Engine, or it 01:05:31 01:05:34 01:05:39 01:05:44 01:05:48 01:05:53 01:05:57

could be the Stealthwatch Management Console. 01:06:00

THE COURT: Is this host shown in the header as the originator of the packet? 01:06:03 01:06:11

THE WITNESS: That is correct, Your Honor. So we're talking about a host on network 1 which, if we're going from network 1 to network 2, would be the source IP address of that header. 01:06:14 01:06:20 01:06:25 01:06:29

THE COURT: Okay. 01:06:33

BY MR. ANDRE: 01:06:34

Q. If we go to Page 979 of this same document, you just testified that it can also send rules to the Stealthwatch Management Console, or SMC. Do you see that? 01:06:35 01:06:43 01:06:47

Describe what is being shown there. 01:06:51

A. Yes. So in this place, just for context, "client" is network 1. You have your switch or router. Your server is network 2. And as the data goes between the switch and router, it's generating log information, and that information goes to Cognitive Threat Analytics, which is Stealthwatch, the Cloud, and then it can send a rule back, the red arrow, which is sending it back to the Stealthwatch Management Console. 01:06:53 01:06:57 01:07:03 01:07:06 01:07:10 01:07:14 01:07:18 01:07:21

Q. If we go to PTX-595 -- 01:07:21

MR. JAMESON: Your Honor, before we go to the next exhibit, I would just note that PTX-1089 is a 4,000-page document, and I just wanted to clarify whether the two pages 01:07:42 01:07:45 01:07:49

that he testified to is what's being admitted, as opposed to the entire 4,000-page document. 01:07:52 01:07:56

MR. ANDRE: That's all we wanted admitted, Your Honor. 01:08:00 01:08:02

THE COURT: Well, as I said, when we deal with a document like that, I want what is admitted to be the relevant pages of the document. If the defense wants to admit other pages of the document, they can, of course, do so. 01:08:02 01:08:06 01:08:16 01:08:25 01:08:32

MR. ANDRE: For the record -- 01:08:35

THE COURT: Assuming that they covered it in their disclosures. 01:08:40 01:08:41

MR. ANDRE: Yes, Your Honor. 01:08:41

And, for the record, we admitted -- we seek to admit Pages 979 and 1238. 01:08:41 01:08:44

THE COURT: All right. 01:08:53

(Plaintiff's Exhibit PTX-1089, Pages 979 and 1238, was received in evidence.) 01:08:53 01:02:56

BY MR. ANDRE: 01:02:56

Q. If we go to PTX-595, Dr. Cole, what is this document? 01:08:55

A. This is release notes for Cisco Stealthwatch. 01:09:01

MR. ANDRE: Your Honor, I'd like to have admitted into evidence PTX-595. 01:09:04 01:09:06

THE COURT: All right. 01:09:21

THE WITNESS: PTX-595 will be admitted. 01:09:21

(Plaintiff's Exhibit PTX-595 was received in evidence.) 01:09:21 01:09:28

BY MR. ANDRE: 01:09:28

Q. If we turn to Page 25 of this document ending in Bates numbers 179, look at the bottom of the page where it says "Change Mitigation Actions." 01:09:28 01:09:33 01:09:41

Can you describe how that influenced your opinion as to generating a rule based on the correlation and provisioning it to a device in the first network. 01:09:42 01:09:44 01:09:48

A. So they're talking about the previous policies -- sorry -- that these have replaced the previous quarantine and unquarantining feature, and you can now apply these policies to the endpoint and change the endpoint authorization status on the network according to the rules and policies configured on Identity Service Engine. 01:09:54 01:09:58 01:10:01 01:10:05 01:10:11 01:10:15

So this is talking about -- the endpoint would be a device on network 1, and it's talking about you can have rules that would take action on a device on network 1, so this aligns very closely with the claim language. 01:10:17 01:10:21 01:10:25 01:10:31

Q. Let me show you one last document before we go back to the claim language, PTX-1018. 01:10:34 01:10:44

And what is this document, Dr. Cole? 01:10:53

A. This is another internal Cisco presentation for Stealthwatch Cognitive Threat Analytics Integration, which is dated January 2017. 01:10:55 01:10:59 01:11:04

MR. ANDRE: Your Honor, I'd like to admit Exhibit PTX-1018. 01:11:07 01:11:10

THE COURT: Just a moment. This is Stealthwatch-CTA Integration. Is this a public document or white paper? What is it? 01:11:14 01:11:24 01:11:35

THE WITNESS: I believe this is an internal presentation that Cisco used and is not public and is proprietary. 01:11:35 01:11:40 01:11:45

THE COURT: All right. 01:11:56

MR. ANDRE: May I get 1018 admitted? 01:11:59

THE COURT: Yes. 01:12:02

(Plaintiff's Exhibit PTX-1018 was received in evidence.) 01:12:02 01:12:03

BY MR. ANDRE: 01:12:03

Q. Turning to Page 11 of this document, ending in Bates number 011, there's a figure of CTA findings. Do you see that? 01:12:03 01:12:06 01:12:12

A. Yes, I do. 01:12:13

Q. Could you inform the Court how this is relevant to your opinion as to provisioning a device with the rules, based on the correlation? 01:12:15 01:12:20 01:12:26

A. Yes. So this shows, if we look at the bottom left-hand corner, based on the analysis that's performed, and if it's escalated and something is critical, then Cognitive Threat Analytics can take action by sending rules that could 01:12:27 01:12:34 01:12:38 01:12:44

quarantine a host on that first network. 01:12:48

And it gives an example here of Identity Service Engine, which is one example, but it also sends it to Stealthwatch Management Console, that would also be on network 1. 01:12:52 01:12:55 01:12:58 01:13:01

Q. Thank you, Doctor. 01:13:02

Could we go back to the claim language and look at this last claim element. 01:13:05 01:13:09

And based on the evidence you provided here today, the testing you've done, the review of source code, and the deposition testimony you reviewed, did you form an opinion as to whether or not the accused Cisco systems infringe the last claim element of claims 11 and 21 of the '176 patent? 01:13:12 01:13:15 01:13:18 01:13:20 01:13:25

A. Just to overview, we started out with the source code that shows it's responsive to correlation. We then went in and showed that there are rules that are created, and then we showed that you can provision a device on the first network, such as the Stealthwatch Management Console. So all these elements of this claim are met, and we can check that box. 01:13:31 01:13:33 01:13:36 01:13:39 01:13:42 01:13:45

Q. Thank you, Doctor. 01:13:51

And now that we've checked all of the claim element boxes for claims 11 and 21 of the '176 patent for the accused switches and routers in combination with Stealthwatch, are you offering an opinion as to whether the accused systems infringe claims 11 and 21 of the '176 patent? 01:13:52 01:13:55 01:13:59 01:14:06 01:14:08

A. Yes. It is my opinion that the infringed routers and switches with Stealthwatch infringe claims 11 and 21 of the '176 patent. 01:14:12 01:14:15 01:14:19

MR. ANDRE: Your Honor, I think now is a good time for the lunch break. I've got one more slight topic to take up with this witness, and we can do it after lunch. 01:14:22 01:14:24 01:14:28

THE COURT: All right. We'll be recessed until 2:15. 01:14:31 01:15:19

(The proceedings recessed at 1:15 p.m.) 01:15:20

CERTIFICATION

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

_____/s/_____

Carol L. Naughton

May 14, 2020